JRC Scientific and Technical Reports

MOBILE IDENTIFICATION:

FROM FUNCTIONAL REQUIREMENTS, TO TESTING FOR INTEROPERABILITY AND SECURITY

Antonia Rana*, Alessandro Alessandroni**
***Joint Research Centre, ****DigitPA**

EUR 25037 EN - 2011

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Antonia Rana
E-mail: Antonia.Rana@ec.europa.eu
Tel.: +39 0332 785478

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 66606

EUR 25037
ISBN 978-92-79-22060-9
ISSN 1831-9424
doi:10.2788/10498

Luxembourg: Publications Office of the European Union, 2011

Printed in Italy

MOBILE IDENTIFICATION: FROM FUNCTIONAL REQUIREMENTS, TO TESTING FOR INTEROPERABILITY AND SECURITY

JRC SCIENTIFIC AND TECHNICAL REPORT

AUTHORS: ANTONIA RANA*, ALESSANDRO ALESSANDRONI**

***INSTITUTE FOR THE PROTECTION AND SECURITY OF CITIZENS, JOINT RESEARCH CENTRE, EUROPEAN COMMISSION**

****DIGITPA**

DATE: 11-11-2011

TABLE OF CONTENTS

TABLE OF CONTENTS **3**

LIST OF FIGURES **4**

LIST OF TABLES **5**

1 INTRODUCTION **6**

1.1 BACKGROUND: FROM MOBIDIG TO E-MOBIDIG 7

2 THE NIST BEST PRACTICE RECOMMENDATION FOR MOBILE ID DEVICES **13**

3 MOBILE IDENTIFICATION APPLICATION SCENARIOS **18**

4 HIGH-LEVEL FUNCTIONAL AND NON FUNCTIONAL REQUIREMENTS **20**

4.1 HIGH LEVEL ARCHITECTURE 20
4.2 FUNCTIONAL COMPONENTS 24
4.2.1 Documents reading *24*
4.2.2 Biometrics enrolment, verification, identification *30*
4.2.3 Data exchange and communication *34*
4.2.4 Optional components *37*
4.3 NON FUNCTIONAL REQUIREMENTS 37
4.3.1 Security of the device *38*
4.3.2 Environmental characteristics *40*
4.3.3 Hardware characteristics of a mobile ID device *41*
4.4 RISK EVALUATION 42

5 TESTING, EVALUATION AND INTEROPERABILITY **45**

5.1 CONFORMANCE TESTING FOR THE DOCUMENTS READING FUNCTIONAL MODULE 47
5.2 CONFORMANCE TESTING FOR THE BIOMETRICS FUNCTIONAL MODULE 55
5.3 CONFORMANCE TESTING FOR THE DATA COMMUNICATION FUNCTIONAL MODULE 64
5.4 SECURITY EVALUATION AND THE COMMON CRITERIA 65
5.4.1 Relevant protection profiles *68*

6 OVERVIEW OF THE SOLUTIONS ON THE MARKET PRESENTED TO E-MOBIDIG **70**

7 CONCLUSIONS AND RECOMMENDATIONS **75**

8 REFERENCES **77**

APPENDIX: ABBREVIATIONS AND ACRONYMS **81**

LIST OF FIGURES

Figure 1: Generic use case diagram for identity verification using document and live biometrics 19

Figure 2: High level architecture for a mobile identification device 22

Figure 3: Activity diagram for mobile identity verification using document and live biometrics 23

Figure 4: Risk management actions as a function of impact and likelihood [IRMF] 44

Figure 5: Test framework 50

Figure 6: Functional components of an inspection system 54

Figure 7: BioAPI framework 58

Figure 8: Steps to certification 68

LIST OF TABLES

Table 1: MOBIDIG subgroups 10

Table 2: Overview of questionnaire outcome 11

Table 3: NIST SAP levels and related standards 15

Table 4: Environmental values for indoor profile 40

Table 5: Environmental values for law enforcement profile 41

Table 6: Reference standard, per OSI layers, for RFID (SCIC) and RFID (PCD) 52

Table 7: ISO/IEC 15408 EAL levels 66

1 INTRODUCTION

Mobile identity and mobile identification are very much talked about concepts nowadays. Evolution in the technology and the trend towards the perceived need to be always able to communicate and interact make mobile identity a fashionable topic. In the security sector, in addition, they respond to the need to be able to perform security checks on identities in non-stationary situations. The terms mobile identification and mobile identity (or mobile ID) seem to have different meanings depending on the context in which they are used. A quick search with Google reveals that "**mobile identity**" is intended in the context of the use of personal mobile devices (such as smartphones) when these devices are used to identify an individual (mostly) to a commercial service. "**Mobile identification**" is slightly different. It yields more result (and already in the first page) instances associated to the use of mobile equipment for identification of an individual from a "third party", involving biometrics and in the context of law enforcement or border control. Some of these results are coming from pilot projects or experiences or devices which have actually been presented in the context of e-MOBIDIG.

In order to avoid ambiguities, in this report, which is associated to the use of mobile equipment to verify the identity of individuals through biometric traits or documents and to the work of e-MOBIDIG, the terminology **mobile identification** rather than **mobile identity** will be used.

The **MO**Bile **ID**entification **I**nteroperability **G**roup (MOBIDIG) initiative started in November 2008 with the **Workshop on Mobile Identity in Europe** organised in Ispra by the Joint Research Centre of the European Commission in collaboration with the French Agence Nationale des Titres Sécurisés. The workshop was attended by about 70 participants from national agencies border control and law enforcement from EU member states and European organisations such as European Commission services and agencies who presented their views and experiences based upon initial trials on the use of mobile devices for identification and authentication of individuals. The workshop aimed at starting a discussion on mobile identification which would address important issues such as best practices in processes and procedures, technical standards, their evaluation in a pan-European harmonised way and interoperability among the different solutions available or adopted. During subsequent workshops, aspects related to the strategy of the working group, to the legal environment in which mobile identification was conducted, to the procedures and processes in practice in the member states and to technical issues were discussed in plenary and in subgroups sessions. The group (whose name was later modified in e-MOBIDIG) also agreed on its terms of references

and on a work-programme and after two years published its first documents on its public website[1]. The documents resulted from the discussions held in the group and are: a strategy document, outlining the strategy of the WG, titled **Identity on the Move—Mobile ID Devices for the future** [22], a document summarising use classes for mobile devices (**e-MOBIDIG Use Cases**) [23], a document containing a summary of the current initiatives on mobile identification in the EU member states (**e-MOBIDIG Country Examples)** [24], a document providing an overview on the technical topics associated to the implementation of mobile identification and authentication solutions **(e-MOBIDIG Technical Guide)** [25] and finally a document describing the standardisation organisation and procedures and standards which are applicable to the mobile identification processes and technologies. The JRC published in 2010 a technical report on the technical challenges in mobile identification [17] which provided an overview of the background, intentions, scope, general objectives and policy context of the MOBIDIG initiative. The report provided also an overview of the security threats drawing from previous work done by NIST [1] and from [50] on biometric systems attack vectors. The present report is a step forward in identifying functional and non-functional requirements and providing a comprehensive overview of the framework for testing and evaluation based on existing standards and references. The purpose is to summarise what has been achieved so far in the fields of (mobile) identification management building on the widespread ecosystem of recommendations, standards, lessons learned and experiences in fields related and applicable to MOBIDIG, taking into account the work and achievements attained so far in an effort to avoid reinventing the wheel and re-invest resources in areas in which results achieved can be re-used.

A brief summary of the MOBIDIG background is provided in the next section, to put the content of this report in context. This summary originates from the various presentations and discussions held in the MOBIDIG workshops in which the authors of this report actively participated.

1.1 Background: from MOBIDIG to e-MOBIDIG

The motivation to start the MOBIDIG initiative aroused from considerations related to the need to employ devices for ***"on-the-move"*** identification of individuals and

[1] The e-MOBIDIG website is at the URL: http://www.e-mobidig.eu

authentication of documents in a variety of applications where the equipment and infrastructure of a stationary environment are not available.

The MOBIDIG group identified possible applications for mobile identification primarily in law enforcement and in border control environments, coming from the experience and expertise presented and described by the various members of the group and invited keynote speakers who participated to the various workshops held since November 2008. The main applications of mobile identification which were identified included:

- Mobile immigration and border control in situations in which stationary equipment would be difficult or impossible to use (e.g. land or sea borders);
- Identification and identity verification in the context of law enforcement in the national territories of member states;
- Identification and authentication for access control to buildings, networks and other access-restricted resources.

The group noted also the need to address standardisation and interoperability aspects in mobile identification to pave the way for successful future interoperability of applications across boundaries, such as, for instance, the ability to inspect national electronic identification (eID) documents from the various EU member states.

It was noted also, in several meetings, that existing procedures and technology for stationary environment could not be directly transferable to mobile environments and that different procedures, including those for testing might be necessary. The need for further analysis and detailed study in this respect was also identified.

The establishment of a working group which could serve as a sort of permanent platform for exchanges of best practices and lessons learned following the approach outlined above would help to solve challenges associated to the use of different technical solutions and to close the gaps between solutions currently deployed and technical evolutions required by changes in the specifications or by technological innovations.

The promoters of the first Mobile Identity for Europe workshop proposed that to ensure these objectives, the WG should[2]:

[2] As presented by the chairman in the first MOBIDIG workshops.

- Identify common European functional requirements,
- Address important issues such as technical standards and security measures,
- Facilitate harmonized testing for compliance to standards, harmonised evaluation and consequently interoperability,
- Provide guidance and recommendations for users and vendors/suppliers.

With the availability of current electronic passports, a mobile identification device would provide for fast identity verification by comparing fingerprints of an individual, acquired on the fly, with the document owner's fingerprints stored in the document chip.

Standards are particularly needed in reading and processing biometric identification traits as data acquired from a device using one system cannot always be read or processed by another system. This may be due to different scanning resolutions, use of images versus templates, use of different image sizes, or use of different fingers. Such a variety of characteristics can have as a consequence a lack of interoperability between systems.

As it refined its terms of reference, MOBIDIG set its objectives in the 4th workshop with the aim to work towards setting a minimum common standards and guidelines on[3]:

- Functionalities and technical requirements and criteria;
- Legal frameworks;
- Procedures and processes;

And towards the establishment of an independent European scheme/infrastructure for:

- Evaluation;
- Certification and

[3] As presented in the fourth MOBIDIG workshop.

- Interoperability testing.

Such steps, similarly to the path taken by ICAO and by the Brussels Interoperability Group (BIG) with electronic passports, would help to achieve industry compliance with established requirements/standards.

MOBIDIG identified and established four subgroups to deal with the elements identified to reach its goals. Table 1 shows the subgroup and the related missions. These were also presented and agreed at the 4th Workshop.

Table 1: MOBIDIG subgroups[4]

Subgroup	**Mission**
Technical	Functionalities, technical and security requirements, standards and criteria; Watching/updating information on technology and security/Testing and certification
Legal	Watching/updating information about legal frameworks; Guidance for legal frameworks
Procedures & Processes	Watching/updating information about procedures and processes, including needs assessment/guidance and best practices; Watching/updating information and guidance on national pilot-projects
Pilot-Projects	Watching/updating information about national pilot projects
Testing and certification	Trials, tests, certification of devices

One of the first initiatives of the MOBIDIG group was to assess the current status in the EU member states regarding mobile identification through a questionnaire distributed to all participants.

The objective of the questionnaire was to collect the necessary data to support preliminary studies/inventories on identification checks. The studies were aimed at bringing awareness on the state of play in identity checks using mobile devices both for

[4] Source: presentation (unpublished) given at the 4th MOBIDIG workshop.

border and law enforcement purposes. The questionnaire contained three sections: one on general information about identity documents, one on pilots in place on mobile identification and a last one on the desirable requirements that mobile identification devices should fulfil both in terms of functionalities and components. The results of the questionnaire, which was completed by representatives of fifteen EU member states are summarised below[5].

Table 2: Overview of questionnaire outcome

Current initiatives in mobile identification
• 8 member states (among those who replied to the questionnaire[6]) are currently using or testing mobile ID devices. • 6 member states use mobile ID devices for border control. • Mobile devices are currently being used by member states for public order police, for criminal police and border police. • 7 member states use mobile ID devices as handheld devices, 6 connect these to a PC, 3 install these in a vehicle. • 10 member states are considering one or more pilot projects before the final acquisition process. • Current initiatives on mobile identification are being carried out by different bodies in different countries (border police, police, civil administration, immigration services). • Interoperability with neighbouring countries is not fundamental.
General considerations
• Devices which combine several functionalities (optical scanning of the MRZ, reading of RFID and smartcards chips, fingerprints and access to remote databases) are already available and in place in some cases. • There is no preference towards the use of commercially available devices or ad-hoc devices. • The fundamental elements in identifying an individual are considered reading an MRZ. Fingerprints can also be important, but legislations are different.

[5] Source: presentations (unpublished) given at the 4th MOBIDIG workshop.

[6] Replies to the questionnaire did not cover 100% of the EU member states.

- Checking the security features of paper documents through a mobile device (e.g. UV and InfraRed) is not considered important. The expertise of the officer does not make mobile different from stationary in this sense.
- In order to access remote databases to look up biographic or biometric information and check watch lists, public (e.g. cellular) networks as well as proprietary ad-hoc networks such as TESTA, TETRA and TETRAPOL are considered equally possible. Additionally, the link should be secured with a VPN.
- As far as the physical/robustness/ergonomics characteristics of the devices are concerned, those considered most important are: resistance against accidental fall, low-high temperature resistance, size and weight, user friendly user-interface (menu navigation) and display, good battery autonomy and autonomy alert and mobile charging facilities

This questionnaire was distributed to a limited audience and detailed results were not published as the work in the MOBIDIG group, which has recently changed its denomination in e-MOBIDIG, took a different direction by engaging a direct dialogue with industry, initially not part of the working group, to examine practical solutions already available on the market.

In order to get an updated view of what is important, what is absolutely necessary and what is useful as well as what is reasonably conceivable given the current experience and state of the art in identification technologies, it could be useful to promote a study which possibly repeats the questionnaire exercise and extend it to a wider audience, possibly including industry.

Even with their limited scope and coverage, these conclusions give a first picture of the functional and non functional requirements that should be taken into account when developing/acquiring a mobile identification solution. Further elements and developments are given in the following sections.

The rest of this document is structured as follows:

Chapter 2 provides a brief overview of the NIST Best Practices Recommendation on Mobile Identification [1], a very comprehensive document on biometrics based mobile identification which sets the standards for the US. Chapter 3 presents application scenarios for mobile identification. Chapter 4 describes the high-level functional architecture and non-functional requirements for mobile identification devices. Chapter 5 covers testing, evaluation and certification and related frameworks and standards currently available. Chapter 6 provides an overview of the characteristics of the devices so far presented to the e-MOBIDIG group and finally Chapter 7 provides conclusion and recommendations to the group.

2 THE NIST BEST PRACTICE RECOMMENDATION FOR MOBILE ID DEVICES

One of the reference documents which should be taken into account when reasoning about needs and requirements for mobile identification is the NIST Best Practice Recommendation (NIST BPR) for Mobile ID Devices [1].

This document, whose architectural classification has already been put at the centre of the system architecture considerations in [17], was published by NIST in August 2009 and is the result of over 2 years work by various stakeholders that included US federal agencies, state and local governments, private sector entities and academic researchers which constituted the Mobile ID ad-hoc work group.

The NIST BPR is focused particularly on the biometric processes for the identification of individuals and on producing a set of guidance principles for the acquisition of biometric components for mobile identification of individuals from their biometric traits, and consider only marginally the use of mobile systems in the authentication and verification of identification documents. The guide contains recommendations on operational requirements for mobile ID devices to be used for biometrics enrolment, identification, and verification functions. In this sense, it has a more limited scope than the one set out for MOBIDIG.

NIST considers a mobile ID device as a ***"portable biometric acquisition station in which captured samples are then compared against samples contained in a local or remote database and, as such it may not consider setups adhering to distance, lighting and other photo-capture standards"*** [1]. This definition sets the context for the establishment of recommendations, guidance and parameters which might be different from those already established and being used in biometrics operations (enrolment, identification and verification) in stationary settings in which controlling those parameters might be much easier.

Taking into account risks and uses for mobile identification devices aimed at covering the cycle: enrolment-identification-verification, the NIST BPR recommendations are tailored to various risk levels categorized according to severity and risks to public safety by suggesting capture application profiles based on that categorization. The aim of the recommendations is mainly to enhance interoperability both between different implementations from different suppliers and with legacy systems.

The NIST BPR defines parameters, content, format and units of measurement for the exchange of biometric sample. Information consists of a variety of mandatory and

optional information items, such as fingerprint scanning resolution, pixel distances between facial features and compression algorithm information. The aim is to make it easier for information captured, compiled and formatted in accordance with the recommendations given in this guideline, to be transmitted and exchanged among different systems.

One of the major problems in achieving interoperability when using biometrics traits for identification of an individual is the lack of standards on templates and on the processes for generating templates[7]. For this reason, in order to ensure the widest applicability, the NIST recommendations focus on the capture, use and exchange of biometric traits (fingerprint, face, and iris are the modalities which are considered) in the form of images rather than templates, as templates would be the result of vendor processed images. In other words using captured images, when data exchange between different heterogeneous systems is required, is the only viable option. When raw images are transferred each of the two systems at the communication end-points will use their own features extraction algorithm independently of the data exchange process.

Following the identified risk levels, the NIST document lists a scale of requirements which becomes more stringent as the risk level increases. This scale is expressed with the concept of Subject Acquisition Profiles (SAP) which identify progressively the set of parameters and requirements relevant for each particular biometric modality. The concept of SAP has its foundations in the type-10 record of the ANSI/NIST standard and has already been described in the context of MOBIDIG in [26]. As the SAP numbers increase, the capabilities of the device increase as well.

In addition to the SAP levels classification, requirements related to biometrics are also examined in the context of the function for which biometrics are used, i.e. for enrolment, identification or verification purposes. The enrolment process is the most critical function from the point of view of the quality and therefore has more stringent requirements. In addition, operational needs of the particular application define the risk level (severe, moderate or mild) and associate these to the requirements outlined in the SAP levels table, which is reported in Table 3.

[7] a biometric template is a set of distinct characteristics that have been extracted from a biometric sample.

Table 3: NIST SAP levels and related standards[8]

	SAP Level							
	5	**10**	**20**	**30**	**40**	**45**	**50**	**60**
Acquire flat images	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acquire rolled images	No	No	No	No	Optional	Optional	Optional	Optional
Minimum resolution	500 ppi +/-10 ppi	500 ppi +/-10 ppi	500 ppi +/-10 ppi	500 ppi +/-10 ppi	500 ppi +/-10 ppi	500 ppi +/-5 ppi	500 ppi +/-5 ppi	500 ppi +/-5 ppi
Minimum gray levels	256	256	256	256	256	256	256	256
Minimum image dimensions (wxh)	.5" x .65"	.5" x .65"	.6 "x .8"	.8 "x 1.0"	1.6 "x1.5"	1.6 "x1.5"	2.5" x1.5"	3.2" x 3"
Minimum image area	.325 sq in	.325 sq in	.48 sq in	.8 sq in	2.4 sq in	2.4 sq in	3.75 sq in	9.6 sq in
Compression algorithm	N/A	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ
Maximum compression ratio	N/A	10:1	10:1	10:1	15:1	15:1	15:1	15:1
Simultaneous number of fingers	1	1	1	1	1 to 2	1 to 2	1 to 3	1 to 4
Sensor certification	PIV	PIV	PIV	PIV	PIV	Appendix F, IAFIS Image Quality Specs[9]	Appendix F, IAFIS Image Quality Specs	Appendix F, IAFIS Image Quality Specs
Minutiae extractor certification	PIV	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Minutiae are the characteristics extracted from images that constitute a template. They are used as interchange format only for SAP5 which is used in the US Personal Identity Verification standard PIV[10] [37]. In this case, PIV is also the standard used for certification while the standard used for minutiae extraction is INCITS 378-2004. In all other cases, the interchange format is the image and the interchange format to exchange fingerprint image information between two systems is ANSI/NIST Type-4 or Type-14. The standard specifies the format of the image and metadata that accompany its exchange such as impression type, i.e. how the fingerprint image was obtained, finger position, scanning resolution, grayscale compression algorithm, etc.

In addition to the detailed requirements given for the biometrics operations, the NIST BPR document includes recommendations or considerations also regarding:

[8] Adapted from [1]

[9] FBI, Electronic Biometric Transmission Specification (EBTS), Ver. 8, 9/24/2007

[10] Personal Identity Verification, http://csrc.nist.gov/groups/SNS/piv/index.html, is the standard used by the US government for identification of government employees.

- device characteristics
- software
- security
- communication settings

From a functional point of view, the NIST BPR partitions the tasks that must be performed by a mobile identification device (image capture, image processing, matching and output decision generation) into the following four steps[11]:

- **Data capture**: the process of acquiring one or more raw biometric samples from a subject;
- **Signal processing**: the process of extracting distinguishing features from a raw biometric sample (image normalisation, feature extraction, quality assessment, template creation, etc.);
- **Matching**: the process of comparing the features extracted from a submitted biometric sample to those of one or more reference templates in a database and generating a resulting similarity score
- **Decision**: the determination of a match/non match conclusion that shall be based on the similarity score meeting or exceeding a specified threshold

These tasks are related to identification using biometrics only, i.e. not taking into account the identification and authentication using electronic documents.

Considering the complete picture for mobile identification which includes, in addition to the mobile device, the back-end system and the communication channel over which the mobile device and the back-end system exchange data and information, these tasks can be distributed in different ways by splitting the workload within a networked system by moving them on the periphery or to the central system. In addition the NIST BPR consider that the final decision regarding acceptability or match of the acquired sample, can be an application decision or an operator decision, i.e. the system might provide the operator with a score and allow him/her the final decision or not.

Regarding the possibility to distribute the workload over the network between the front-end (the mobile identification device) and the backend (the remote, back-office system), the NIST BPR identifies four possible architecture scenarios:

[11] Also extensively described in [17].

Scenario 1: Data capture, signal processing, matching and decision are performed on the mobile ID device. This scenario does not require any network connection and is conceptually and technically very simple, however it requires a local copy of databases which might not be feasible for legal reasons in every country.

Scenario 2: Data capture, signal processing and matching are performed on the mobile ID device, but the final decision is taken remotely. This scenario requires a network connection which links the mobile device to the decision making module.

Scenario 3: Data capture and signal processing are performed on the mobile ID device, while matching and the final decision are performed remotely. This scenario requires a network connection which links the mobile device to the matching and decision making module.

Scenario 4: Only Data capture is performed on the mobile ID device, the captured raw biometrics is then transmitted to a remote server which elaborates the image and extracts features, matches the extracted features against a database and takes the final decision. This scenario requires a network connection which links the mobile device to processing remote server which all processing operations.

Examples of factors influencing this architectural decision are: availability of network connectivity, bandwidth of the network connection, need to be interoperable with existing or legacy systems, etc.

The NIST BPR concludes by offering guidance on the physical characteristics of the device according to three possible usage scenarios:

- Indoor scenario
- Law enforcement scenario
- Military scenario

The most relevant from them are discussed in the section on non-functional requirements.

3 MOBILE IDENTIFICATION APPLICATION SCENARIOS

The e-MOBIDIG document on Use Cases [23] provides a comprehensive overview of the classes of use for mobile devices. Mobile devices are classified into 5 classes:

- class1: handheld devices
- class2: car-based mobile systems
- class3: biometric enrolment
- class4: mobile office
- class5: non-government identity authentication

Each one of these classes is further divided into cases that further classify possible usages of the mobile devices within each class.

The present section complements the information provided in [23] by taking into account the various discussions and considerations developed during the two years of e-MOBIDIG work and mentioned in the first section of this report, and possible application scenarios for mobile identification and by providing a diagrammatic representation of the application scenario process.

We can identify two broad-level application scenarios:

> **Application Scenario 1**: Acquisition of biometric, biographic and other information (e.g. car plate identification) and check against information in remote (or local) databases.

This scenario applies to law enforcement rather than to border checks. This is the main application that is covered in the NIST BPR document which mentions documents checks only marginally and focuses on the match of live biometrics against remote databases. Additional information acquired in this scenario could be the car number plate.

This scenario requires data communication connection for access to remote databases against which information captured live will be matched or otherwise local copies of the databases on the mobile device.

> **Application Scenario 2**: Acquisition of biographic information from electronic documents, acquisition of biometrics, authentication of the document.

This scenario does not necessarily require access to remote databases as in principle the document can be used to check the identity of an individual by verifying the information contained in the chip against the biometrics captured live.

However, this scenario might require access to the certification infrastructure for certificates and signatures validation (both CSCA/DS for passive authentication and CVCA/DV for EAC). An alternative solution would be to load the necessary certificates and certificate revocation lists at the end of a shift once the device is brought back to the office and can be updated. The decision on the solution to be adopted involves technical as well as legal considerations and might differ according to the country. This should be considered during a risk assessment process.

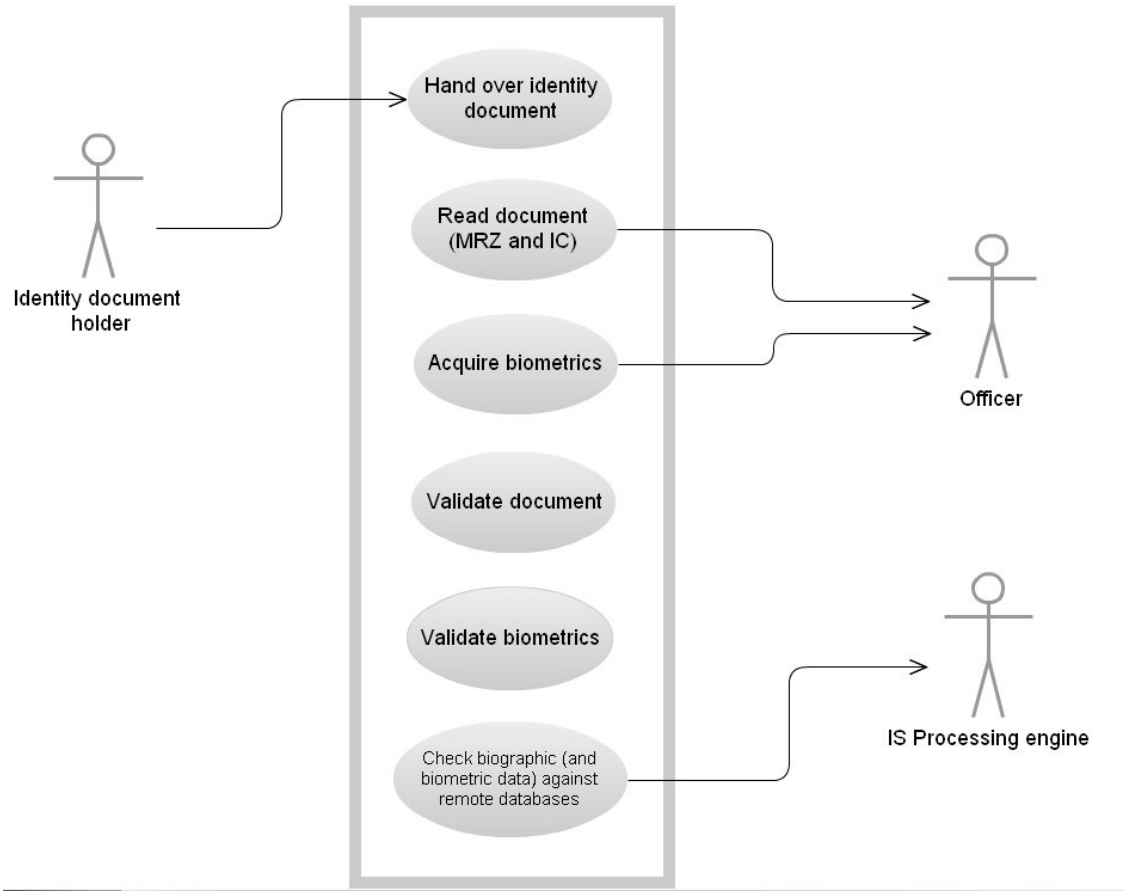

Figure 1: Generic use case diagram for identity verification using document and live biometrics

4 HIGH-LEVEL FUNCTIONAL AND NON FUNCTIONAL REQUIREMENTS

This section will discuss the high-level architecture of a mobile identification system, outlining the main components, the functionality that they provide and a set of characteristics which they should possess which are not related to functions but rather to environmental constraints or security requirements. The contents of this chapter originated from the discussions within the technical subgroup of MOBIDIG.

4.1 High level architecture

The information gathered so far from previous work and the analysis of the application scenarios, allow us to identify the high level functional components of a mobile identification solution.

Basically, the functional requirements are similar to those of a stationary systems plus additional consideration for restrictions of mobile devices and related to data communication and associated security measures.

The initial work of the technical WG of MOBIDIG identified the following capabilities which would be desirable:

Document verification in mobility:

- Verification of the document authenticity (security features);
- Reading of the Machine Readable printed information from the document (for example an ICAO compliant MRZ or a barcode);
- Reading the content of the contact or contactless chip of the document;
- Verification of the chip authenticity and integrity of the data contained in the chip;
- Capturing the biometric samples (fingerprint or face) for the purpose of performing a 1:1 identity verification between the captured sample and the sample stored in the document chip or in a remote database;
- Capturing the biometric samples (fingerprint or face) for the purpose of performing a 1:N biometric identification in a local or remote database;

- Querying of centralized databases, for the purpose of checking if a document has been reported as lost or stolen or present in a black-list .

Clustering the desirable functional capabilities according to the identity element they operate on (e.g. to an electronic document) we can summarise that a mobile identification solution must support:

- Verification of identity documents
- Access to biometric data on RF chips
- Biometric identity verification
- Connection to background systems

which allows us to identify the following high level system components (Figure 2):

- Document reader, capable of optical reading (e.g. MRZ line), RF communication and of accessing data on the IC
- Biometric capturing and matching device;
- Computing platform, application engine and user interface;
- Secure data communication for access to remote databases

From a hardware point of view, the devices providing these functional capabilities can either be integrated in one single device or consist of independent components connected to each other, which communicate with each other either via short-range radio communication (e.g. Bluetooth) or via wired connection (e.g. USB or proprietary). The choice of the particular hardware solution can be dependent on the application scenarios in which the device(s) will be used, on the need to take into account legacy systems and on physical constraints such as:

- Total weight of the device/devices;
- Usability;
- Total cost;
- Availability of existing legacy computing and communication devices (such as computing and communication platforms mounted on patrol car, PDAs, etc.).

During past MOBIDIG workshops several solutions currently being implemented in pilots or in operational settings in some EU member states have been presented. The range of

solutions currently in place is large. In order to benefit from lessons learned in deploying solutions based on the use of these devices, MOBIDIG could prepare a questionnaire to gather information and experiences taking into consideration homogenous factors which could be useful in drafting a set of recommendations. The Country Examples document [24] is a step towards this direction, however information presented in that document has different levels of details which make it difficult to get a homogeneous overview of the current situation both from process and technical viewpoints. A further step should be taken in the direction of modelling the information provided therein in a more structured and categorised manner in order to provide more efficiently a homogeneous overall view which could be useful for further processing.

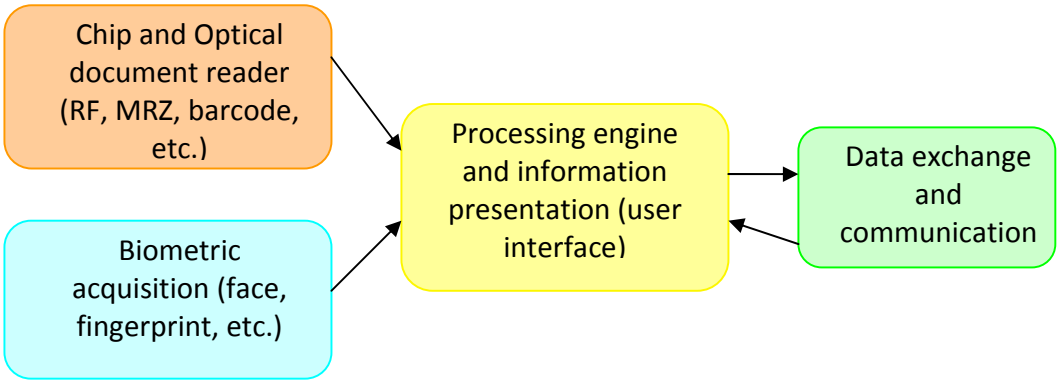

Figure 2: High level architecture for a mobile identification device

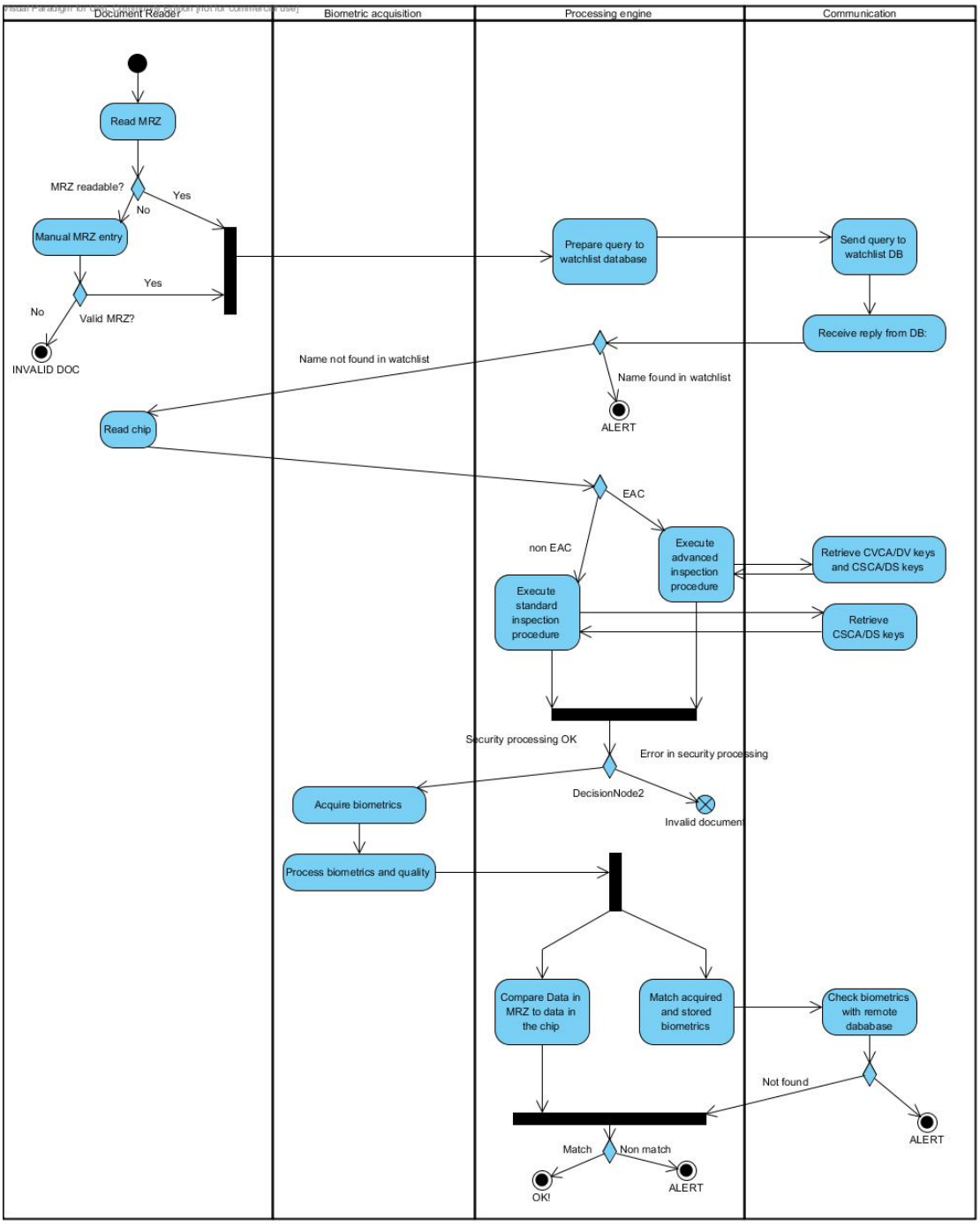

Figure 3: Activity diagram for mobile identity verification using document and live biometrics

4.2 Functional components

As outlined in section 4.1, we can identify four main functional components in a mobile identification system:

- Document reading
- Biometrics enrolment, verification, identification
- Processing engine, data entry and information presentation
- Data communication

Additional optional functional components might be considered according to "local" requirements.

These components are briefly described in the following sections.

4.2.1 Documents reading

The document reading component is the most important functional component for border control applications in which identity verification involves use and authentication of a travel document.

Depending on the application scenario, this component might be required to be able to read different types of documents, in general all documents which can be accepted as ID document. As a minimum, the document reading component should be able to read the EU electronic passport and the new EU residence permit card.

More in detail, in order to be able to authenticate electronic passports and residence permits, the document reading component should be able to:

- Read the machine readable information printed on the document according to the ICAO specifications [4];
- Read the content of a contactless chip, according to the specifications ISO/IEC 14443A/B [14], [15] and [16];
- Engage in the security protocols implementing the ICAO security features and access control;
- If the passport chip requires it, engage in the EAC security protocols.

Part of these functions will be performed in the reader, those functions related to the OSI upper layers (access to data, security) might be performed in the processing engine component.

In order to verify the chip authenticity, extract the data stored in the document chip and verify the integrity of the data, the following security features and protocols should be implemented:

- Basic Access Control as defined in [4];
- Extended Access Control as defined in [19].

With the third generation of ePassports, a new security mechanism Supplemental Access Control (SAC) [30], based on Password Authenticated Connection Establishment (PACE v2), is introduced to overcome the weaknesses of BAC. The ICAO and the European Union have recently decided to enforce the use of this protocol for all ePassports and eResidence Permits to be issued as of 2014, therefore the reading devices must be updated to support SAC.

ICAO Document 9303 [4] specifies the standards an ICAO conformant ePassport or Residence Permit card must be complied with. The standardisation element is the electronic document. Similar specifications documents are not available for reading or inspection system devices. However, reading and inspection systems devices are the communication counterparts of documents and, in fact, must be able to "speak the same language". ICAO and the EU promoted so called interoperability events in the past in order to provide the opportunity for document and inspection systems producers to sit together and test the interoperability of the components-devices at the two ends of the communication channel. In order to facilitate preparing for the interoperability events, the ICAO published a ***Guide to Interfacing e-MRTDs and Inspection Systems*** [49] already back in 2005 which, extrapolated from [4] the requirements on the inspection systems (including both the reader and the inspection system layer 6-7 processing functionalities).

The guide lists the functional specifications that an inspection system should provide in order to achieve global interoperability in reading ePassports and, more in general, electronic machine readable travel documents (eMRTD).

Such indications were given following the findings of the ICAO tests in order to improve global interoperability and do not constitute an official requirements document. In fact, the guide is no longer available on the ICAO website. Nevertheless, the guide still contains important indications to make sure that different vendors implementation of the standard are capable of working together.

The requirements are divided into physical, security, MRZ, speed, communication protocols, IC data, data authentication, algorithms, and access method and. Those which are more relevant also for mobile equipment are summarised below:

Physical requirements:

- Capability to accept oversize passports (page size 9 cm. x 14 cm);
- Use of the reader should not require knowledge of reader antenna location;
- Should provide visible indication of power and status (e.g., offline, ready, processing);
- The reader design should enable reading of the contactless chip without requiring repositioning of the document in open and closed book configurations;
- Should be capable of exporting biographic data read both from the MRZ and from the IC contactless chip.

Security requirements:

- Should be designed to inhibit eavesdropping of communications with the contactless IC chip from a distance greater than 1 m from the reader;
- Should be designed to inhibit jamming of reader operations from a distance of 30 cm from the reader.

Machine Readable Zone requirements

- If a contactless chip messaging session fails, the inspection system should be able to re-initiate a session without requiring re-reading of the MRZ;
- The inspection system must be capable of exporting the MRZ data and correct it when a failure with BAC occurs and to open the chip once the MRZ data is corrected.

Speed requirements

- Reader initialization must take less than 2 seconds.
- Retrieval of data from chip must take less than 2.5 seconds for IC chips with 32k of data and less than 5 seconds for IC chips with 64k of data.

- Polling/Interaction response must occur within two seconds from placement of chip on reader.

Communication protocols requirements

- Inspection systems must support both ISO 14333-A and 14333-B protocols and anti-collision processes identified in ISO 14333;
- The field strength values must be such that readers' antenna prevents interferences with other electronic devices within 30 cm and prevents capture of IC chip data from a distance greater than 10cm.

Data requirements

- Inspection systems must be capable to retrieve at least DG1 and DG2 which are mandatory for eMRTDs. Retrieval of data in additional data groups (DGs) is optional and a choice of the country implementing the inspection system;
- Inspection systems must be able to retrieve both JPEG and JPEG2000 images from DG2 since either JPEG or JPEG2000 are allowed on eMRTDs.

Data authentication requirements

- Passive authentication is mandatory for eMRTDs, inspection systems must be able to verify the authenticity and integrity of the data stored in the chip by performing the passive authentication protocol using the security data object, its signature and the country signing certificate.
- Active authentication (AA) is optional for eMRTDs and in EU effectively replaced by chip authentication (CA) which is part of EAC. The ICAO guide does not contain any recommendation regarding AA, however, for EU second generation passports, the IS must be capable of executing the CA.

Algorithms requirements

- Inspection systems must support RSA and ECDSA.
- While ICAO recommends that signatures are generated using RSASSA-PSS, inspection systems must be able to verify signatures generated using RSASSA-PKCS1-v15
- Inspection systems must support the SHA-1, SHA-224 and SHA-256 algorithms

Access control

- While BAC is optional for ICAO, inspection systems must be able to support it in order to be able to access BAC- equipped eMRTDs.
- With the entry into operation of SAC in the EU in 2014, inspection systems must be able to support PACE v2 in order to access SAC-enabled eMRTDs.

Being a document which needs to be "read" worldwide a lot of effort was put by international organisations in developing a standard for electronic machine readable travel documents, including the electronic passports. A lot of experience was also gained on the practical issues with several interoperability testing events. As a consequence, requirements for document reading when the document used for identification is an e-MRTD are rather well established.

The status is different for other types of documents which might be used to verify individuals' identity using mobile devices. This is because international specification might not be available, specifications might be issued on a national basis and not published, and therefore reading might be restricted to the country in which the document is issued.

Without considering the semantics associated to the way information is organised and to what information is contained in an electronic document (this is the topic of the PORVOO group for eID cards, for instance), from the purely hardware point of view, other functionalities that might be implemented in the documenting reading component in order to be able to read other types of documents, might include the capability to read:

- 1-D or 2-D barcodes
- Contact-based smartcards implementing the ISO 7816 specifications (these are used in some ID cards issued in EU member states)

Similarly to reading electronic passports and residence permits, the functions which implement the upper OSI layers might be implemented in the processing engine component.

Implementing the functionalities required to read and authenticate an electronic passport is the minimum level for interoperability. In order to enable reading of other types of electronic documents, it will be necessary to have publicly available specifications for the operating systems, data structures and security measures defined

for that particular document. This is true for electronic ID cards, for electronic driving license, or any other type of electronic document which might be used and accepted as an identification document. If these are not available, it is difficult to talk about interoperability.

Interoperability or the capability to read electronic ID cards might be easier if a common standard is adopted by countries which would like to have electronic document cross-border interoperability. One example of such standard is the CEN set of standards on the European Citizen Card, i.e.:

CEN/TS 15480-1:2007 - Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics

CEN/TS 15480-2:2007 - Identification card systems - European Citizen Card - Part 2: Logical data structures and card services and

CEN/TS 15480-2:2007 - Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface which specify the Electronic Citizen Card (ECC) requirements.

Reading from the CEN website presentation of this standard: *"The ECC, is a smart card issued under the authority of a government institution, either national or local and carries credentials in order to provide all or part of the following services: 1) verify the identity; 2) act as an Inter-European Union travel document; 3) facilitate logical access to e-government or local administration services.... The requirements described in this Technical Specification are used to: a) define a plastic body card with associated physical and logical securities; b) specify the electrical interface and data transport protocols for the ECC; c) support the basic set of Identification and, authentication elements visible at the card surface. This Technical Specification also contains a possible methodology for ECC durability testing in informative Annex B. This Technical Specification refers to the European legislation and regulations in effect."*[12]

The ECC standard very modular, it consists of a framework in which **profiles** represent use-related functionalities such as eGovernment services or travel document application, which is compatible with the ICAO specifications. Countries implementing the ECC specifications can select the components most suited to the national applications. France is one of the countries implementing the ECC specifications for their eID card selecting a profile, known as IAS-ECC which includes two applications: e-travel, supporting the ICAO LDS, BAC and EAC and communicating via a contactless interface

[12] http://esearch.cen.eu/esearch/extendedsearch.aspx

and the e-Administration application providing authentication and signature services and communicating via a contact-based interface.

The European Network and Information Security Agency (ENISA) published in 2009 a report on ***Privacy Features of European eID Card Specifications*** [36] which contains an overview of ID Card Schemes in the European Economic Area and references to the electronic ID cards specification of EU member states where they are available. Although the document is focused on privacy issues, it contains some information about overall functionalities and interfaces and provides an overview on characteristics and differences among national solutions for an identification document which, in many cases, is also a valid travel document. Being able to access its data for identification is useful both in law enforcement and in border security applications. Additional information on national electronic ID cards in EU member states is contained in the IDABC report ***Analysis and Assessment of similarities and differences – impact on eID interoperability*** [51]. A reader component that is capable of reading also identity information from eID tokens provides much larger applicability while requiring from a hardware point of view most probably only a contact-based interface. However achieving interoperability at the semantic and syntactical level (the data and how it is described) as well as at the level of the security and privacy measures is not a trivial task.

4.2.2 Biometrics enrolment, verification, identification

The second component in the high level functional architecture is the Biometric acquisition. This component contains all the functionalities necessary to implement the biometric related functions, i.e. enrolment (biometric acquisition), identification and verification and consists primarily of the two subcomponents:

- A hardware sub-components to capture biometric data, e.g.:
    - Fingerprint scanner
    - Camera to capture facial images
- A software sub-component to perform the matching functions, which comprises:
    - Quality control software: to check the quality of the acquired biometric trait. [2] is the most commonly used.
    - Image compression and decompression functions: If a biometric sample is captured for the purpose of transmitting it to a central system, it is necessary to compress the raw image to optimize its size for transmission. In the case of a fingerprint, the image can be compressed

by using the WSQ or JPEG2000 algorithms, while a facial image can be compressed using JPEG or JPEG2000.

- Algorithms for biometric matching: This function is performed locally when 1:1 matching of the live biometric trait with the biometric trait stored in a document is required. This component must be able to perform the following functions:
  - To extract features from the acquired and stored raw image;
  - To decompress the compressed biometric sample stored in the document chip;
  - To perform the 1:1 matching between two extracted feature sets.
  - All these functions can be performed either in software or by a specialized hardware module embedded in the device.

The ability to process biometric data with good quality is particularly important for mobile devices as these run, in most cases, on less powerful computing platforms such as PDAs or smartphones. This is because processing biometric images requires optimised biometric algorithms which in turn require adequate processing speed and memory in the processing engine. Results can be optimised if the quality of the captured images is good.

In general, we can observe the following characteristics associated to implementing biometrics processing in a mobile identification device:

- The capture devices are smaller, sometimes low quality. This has positive impact on weight and cost but a negative impact on accuracy.
- Limited processing power might result in implementing lighter versions of encoding and matching algorithms. In this case, tests comparing performance would be useful.
- Quality assurance and compression software and their consequences on: performance (FAR, FRR, FTE) and interoperability might result in lower accuracy and higher error rates. Performance test studies would be helpful to assess this aspect.
- Tests on performance could help in setting guidelines to harmonise the performance of mobile and stationary border control systems (FAR, FRR, FTA, number of attempts, number of fingers used)

The NIST BPR [1] recommends that, independently of the location of the matching process (which can be done locally or on a remote server, particularly in the case of comparing against a database), an initial image quality assessment should be done locally, in order to provide feedback to the operator during the capture process who can therefore repeat the acquisition if the quality is not good enough. NIST recommends that the system should use the NFIQ algorithm [2] and should alert the operator if a poor fingerprint image was captured (corresponding to NFIQ level 4 or 5), in this way, acquisition can be repeated to capture an improved image.

The NIST BPR gives also detailed indication on the parameters that should be considered in acquiring good quality biometric images for fingerprints, face and iris. The parameters considered by NIST for fingerprint and facial image are summarised in sections 4.2.2.1 and 4.2.2.2, without specifying the values that NIST suggests. The reader is referred to the original document for a detailed description of the parameters and associated values. The intention of listing them here is to give MOBIDIG the opportunity to discuss on the range of values which would be appropriate for the EU application scenarios, while still working on a set of parameters which have already been discussed among an expert group of stakeholders as being the most relevant.

4.2.2.1 Fingerprint capture requirements

The most relevant parameters that should be considered for fingerprint biometrics are outlined below. The definition of the appropriate value for this parameters is influenced by the verification function that it applies to (enrolment, identification or verification) and by the need to exchange data with other systems.

- Minimum acceptable scanning resolution
- Minimum image dimension (width x height)
- Compression algorithm
- Compression ratio
- Sensor certification (e.g. FBI's IAFIS Image Quality Specifications certification) [35]
- Minutiae extraction certification. This applies only in those cases when minutiae exchange vs. image exchange is accepted, in this case the NIST document specifies that INCITS 378-2004 minutiae data format standard should be used. ISO/IEC 19794-2:2005 is another international reference standard for the format of minutiae that can be used. This parameter is not relevant in case biometric processing involves checking the biometrics in an electronic passport, as in this case images and not templates of the captured biometrics are stored.

According to a systematic experimentation carried out by University of Bologna the most critical quality parameters are the image dimension and the output resolution accuracy which, at the PIV IQS minimum requirements, may cause a reduction in performance in terms of lower accuracy of 73% and 20%, respectively, compared to the performance that can be achieved using a device of area equal to one square inch (25.4 x 25.4 mm) and 500ppi±1% output resolution [32]. The size of the fingerprint image according to the PIV standard is 12.8 x 18.0 mm corresponding to the NIST SAP 10 level.

4.2.2.2 Facial image capture requirements

Capturing facial images might be particularly important for assessing the authenticity of an electronic document which stores a digital image of the face such as the electronic passport, or in checking the facial image against a database.

As it is the case for fingerprint, also for facial images a captured image could be used for two distinct purposes:

- **Verification**: i.e. 1:1 match such as in checking that the person matches with the picture stored in the passport chip. In this case, the NIST BPR suggests that low-resolution cameras with fixed focal length provide sufficient data for linking the return information to the subject.
- **Identification**: i.e. 1:m match such as using the captured facial image picture to search against a database of other facial images. In this case higher-end camera features are required.

Depending on the application, acceptable range values for the following parameters related both to capture and interchange requirements, should be defined:

- Capture distance
- Capture device control (manual or automatic, help to take quality pictures in bright sunlight, overcast light, indoors, etc.)
- Photo image format (for facial recognition colour images should be used)
- Capture device image size and aspect ratio (the NIST document refers to [3] for specifications related to this parameter)
- Capture device sensitivity
- Facial image compression (the NIST document refers to [3] for specifications related to this parameter)
- Standards used for additional metadata (if metadata such as device sensor, capture distance in mm, illumination type, exposure type, etc. should be

exchanged as well, relevant standards for the exchange of this type of information such as [3] should be used)

As for fingerprints, an initial image quality assessment should be done to provide feedback to the operator during the capture process. Unfortunately, for facial images, no standardised algorithm is broadly available that would help system interoperability between different systems.

4.2.3 Data exchange and communication

There are two aspects related to the data communication component: the first one is the "local" communication between device subcomponents in the case the mobile identification solution consists of several integrated sub-components. The second one is the remote connection to the central system or systems where the back-end databases are located. Although the two cases use different technologies and can benefit differently of wired connections, considerations on performance and security level apply to both.

Aspects that need to be considered when talking about data communication are:

- **Data exchange format**: this is particularly relevant if access to different databases is foreseen. It is fundamental that data, especially biometric data, is formatted in a way that is "understood" by the receiving end. Data exchange can be facilitated by using a standard data description such as [3];
- **Bandwidth**: bandwidth must be both reliable and sufficient to send data and receive response in "reasonable" time;
- **Security**: although a layered approach to security can be implemented by adding encryption capabilities at the application level (e.g. by using a VPN, SSL or TLS tunnel, etc.), it is important that the network link itself has some encryption capabilities, in order to be able to deploy a layered approach to security;
- **Network coverage**: when public networks are used, it is important that areas in which the mobile devices will be used are sufficiently covered.

Possible public communication long-range networks are identified below. Details about some of these network links are already given in [26] and therefore for these cases, a description of their features will not be repeated in this document.

4.2.3.1 Cellular connectivity

Possible public communication long-range networks are:

- GSM/GPRS– data rate around 40 Kbps
- EDGE/UMTS - – data rate up to 1Mbps
- HSDPA/WCDMA – data rate projected to reach 40 Mbps

In the context of cellular communication, 4G, the forthcoming fourth generation of cellular wireless standard, promises to be the optimal solution in terms of throughput and security, providing a comprehensive IP-based solution where voice, data and streamed multimedia are integrated.

The term 4G comprises a number of standards being defined by ITU-T. Technologies which are being considered pre-4G are: WiMax, WiBro, iBurst, 3GPP Long Term Evolution (LTE) and 3GPP2 Ultra Mobile Broadband.

In addition to commercial communication services, the following private communication long-range networks are available:

- Tetra
- Tetrapol

More information on these protocols is given in [25].

4.2.3.2 Satellite communication

Satellite communication could be an option if cellular communication is not available. However use of satellite communication devices is less practical as most satellite communications require bulky transmitters/receivers. Mobile ID devices can communicate with these devices using cables or Bluetooth connections.

4.2.3.3 Wireless connectivity

The term “wireless connectivity” in fact includes all wireless technologies and therefore also cellular and satellite. Often this term is used to indicate WiFi wireless communication which include all the technologies implementing the standard IEEE 802.11 including 802.11a, 802.11b, 802.11g and 802.11n. WiFi is a wireless local area network which is easily connected to the internet via access points connected to DSL or LAN networks. WiFi connections are practically provided in all mobile identification devices based on PDAs or smartphones. WiFi connections provide several levels of security through encryption of the communication channel. The most secure is considered nowadays to be WPAv2 (WiFi Protected Access version 2), which encrypts

the data using the TKIP (Temporal Key Integrity Protocol) encryption protocol with a 128-bit per-packet key.

4.2.3.4 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication that is used to connect various types of consumer devices, from cellular phones, to laptops, automobiles and headsets in a Personal Area Network. The standard has been revised and updated several times. The current version is 2.1+EDR (Extended Data Rate). It provides faster transmission rates and significant security improvement.

According to discussions in MOBIDIG workshops, Bluetooth is the technology of choice in most cases in which multi-component solutions are chosen for mobile identification. The security of Bluetooth communications has been the subject of many scientific papers (as for other network protocols). But for the Bluetooth protocol there is also a guideline from NIST regarding its security and secure usage [21]. Bluetooth technology and associated devices are susceptible to general networking threats such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification and resources misappropriation. Literature also reports about threats which target vulnerabilities specific to the Bluetooth protocols and some implementations which exploit these vulnerabilities are available on the internet. Attacks against improperly secured Bluetooth implementations can provide attackers not only with unauthorised access to sensitive information but also to with access to other systems or networks to which the compromised devices are connected.

Without entering into the technical details, the following recommendations, among those contained in [21] are in particular useful when connecting devices via Bluetooth which are security or privacy sensitive.

Use the strongest security mode available

The Bluetooth specifications define four security modes, which offer varying levels of authentication and encryption (authentication in Bluetooth refers only to the authentication of the device, not of users using the device). Security Mode 3 is considered the strongest mode because it requires authentication and encryption to be established before the Bluetooth physical link is completely established. Security Modes 2 and 4 also use authentication and encryption, but only after the Bluetooth physical link has already been fully established and logical channels partially established. Security Mode 1 provides no security functionality.

Address the specific security requirements regarding usage in the security policy

The policy should include a list of approved uses for Bluetooth, a list of the types of information that may be transferred over Bluetooth networks, and requirements for selecting and using Bluetooth personal identification numbers (PIN). In the case of use of Bluetooth for law enforcement or border control use, a centralized security policy management approach seems more appropriate.

4.2.4 Optional components

Additional components that might be considered in order to achieve a mobile identification are automatic number plate recognition and geographic positioning. **Automatic number plate recognition** (**ANPR**) uses optical character recognition on images to read the license plates on vehicles and search reference system for lost and stolen vehicles in local or central databases or even to identify individuals from a remote biographical database if an identity document is not available.

Other optional functionalities could be:

- capturing the device geographic position (GPS) for the purpose of geotagging the captured information and/or transmission of the device position to a central system for position tracking and monitoring;
- capturing multimedia information (still images, videos, audio, text notes) with option for local storage and transmission to remote system.

4.3 Non functional requirements

Non functional requirements include all characteristics that a mobile identification solution should possess which are not related to the identification functionality but rather to the management and administration of the device, to its security or to the usability/ergonomics or environmental requirements. Usability and ergonomics are particularly important for devices which most probably have to be worn on a belt in addition to other devices for a whole shift and must be handled easily and efficiently while interacting with the individual being identified.

The most important requirements in this respect are already clear from the first discussions held within the e-MOBIDIG group.

Other non-functional requirements could include elements which are related to the infrastructure environment or capabilities in the service which is going to use the equipment and to the architecture of the complete application (i.e. the distribution of the signal processing and matching functions over the network or to remote servers). Typical examples in this sense are the operating system platform, the choice of which might be influenced by the current or legacy environment or by the availability of suitable algorithms for quality and matching of biometric samples and the computing power/main memory which are greater when heavier local processing is foreseen in the application.

4.3.1 Security of the device

By security of the device we intend the measures put in place to protect the mobile devices against loss, theft and misuse which could potentially result in authorised access to information or databases.

Security of the device depends on a mix of policies and technologies. Policies identify the measures that should be adopted and the technologies that will be deployed in order to implement them. Security policies should specify how confidentiality and integrity of the data transmitted to and from the device and of the data stored on the device are ensured. Policies should include measures regarding authentication of the operator to the device and of the device to services, data erase, data encryption, application launch controls and disabling device feature.

Security of the device is addressed in the appendix of the NIST BPR as an important issue but not part of the recommendations body.

While no standard can be defined in this sense, since these measures are associated to local management and to the definition of a local security policy, identifying common aspects and recommendation can be useful in achieving comparable levels of security.

Key issues that must be addressed while establishing a comprehensive security policy for mobile devices include:

Encryption of data on the device: measures might be related both to main memory and particularly to storage cards where they are used. The security policy should establish which algorithms, key lengths and key distribution procedures will be used. These are “local” decisions as they will not affect in any way interoperability of readers vs. documents or biometrics images vs. remote databases. Standards and associated

certification schemes do exist which can help and should be considered. Examples of such standards are FIPS 140-2, ISO/IEC 19790 and ISO/IEC 24759[13].

Encryption of data transmitted from the device to the remote servers and vice-versa: similarly to the previous case, the security policy should establish which algorithms and key lengths should be used. In addition key distribution procedures should also be defined.

Data integrity: data integrity ensures that data is not modified. The security policy should establish which algorithms will be used for data stored on the mobile device.

Operator authentication: the security policy should specify the measures that will be taken to authenticate the mobile device operator. Two-factors authentication schemes (i.e. token+PIN, biometrics+PIN, biometrics+token) are more secure. Security measures related to operator authentication include also specification of the idle-time after which re-authentication is required, and the maximum number of failed authentication attempts before the device clears all data or is locked. E-MOBIDIG could establish some guidelines on this respect following the best practices and lessons learned from the current ongoing pilots in the EU member states.

Device authentication: the security policy should also specify the mechanism that the device uses to identify itself to the remote servers. These measures might, in fact, depend on the requirements of the remote service being accessed. In relation to device authentication, the security policy should specify whether black lists should be consulted and which. A special type of device authentication is also required by the Extended Access Control if the EAC protocol and its Terminal Authentication protocols are implemented.

Policy, software and certificates updates: finally, the security policy should specify the software updates procedures and the procedures for uploading certificates needed by

[13] FIPS 140-2, Security Requirements for Cryptographic modules specifies security requirements for a cryptographic module utilised within a security system protecting sensitive but unclassified information. It provides four increasing qualitative levels, which are aimed at covering the wide range of potential applications and environments in which cryptographic modules can be employed. The standard is complemented by the Cryptographic Module Validation Programme operated by NIST which validates compliance to the requirements.

ISO/IEC 19790 Information technology - Security techniques - Security requirements for cryptographic modules, which is derived from NIST Federal Information Processing Standard (FIPS) PUB 140-2, Security Requirements for Cryptographic Modules.

ISO/IEC 24759 Information technology - Security techniques - Test requirements for cryptographic modules which was derived from NIST Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

passive authentication and EAC in electronic passports or analogous certificates which might be required for other types of documents.

4.3.2 Environmental characteristics

Requirements for resistance against environmental factors were also included in the questionnaire mentioned in the first section of this report and are also considered in the NIST BPR. Different usages require different levels of resistance to the environmental factors such as temperature, humidity, dust, water, vibration, etc which will depend on the expected usage and the location where they will be required to operate.

The NIST BPR identifies three profiles and a number of factors common to the three profiles (operating temperature, storage temperature, relative humidity, Ingress Protection rating) plus additional specific factors for profiles with more stringent requirements.

The first profile identified is called **indoor profile**. The characteristics of this profile are assumed to be similar to those provided by most commercially available computing devices.

The low-high end range values for this profile are summarised in Table 4[14].

Table 4: Environmental values for indoor profile

Operating temperature	0 +40 C
Storage temperature	-10 +50 C
Relative humidity	Max. 85% non condensing
Ingress Protection rating (IP Code)[15]	IP 40 or higher

The second profile is the **law enforcement profile**. In addition to the parameters identified for the indoor profile an additional requirement is added on drop resistance:

[14] Tables in this section on environmental profiles are adapted from [1].

[15] IP Codes are defined in IEC 60529, "Degrees of Protection provided by Enclosures (IP Codes)," ed. 2.1 (Geneva: International Electrotechnical Commission, 2001).

Table 5: Environmental values for law enforcement profile

Operating temperature	-10 +50 C
Storage temperature	-20 +60 C
Relative humidity	10-90% non condensing
Ingress Protection rating (IP Code)	IP 54 or higher, in operational configuration, with any existing expansion port closed
Drop resistance	Resistance to multiple drops on concrete from a height of 90 cm

Finally a military profile is identified in which an increased level of protection against low/high temperatures and protection against dust and sand, rain, water splashes, vibration and drops are defined.

4.3.3 Hardware characteristics of a mobile ID device

As already mentioned previously, the hardware characteristics of the device must be such that the computing platform is able to support the software applications that will run on the device. The following components have to be considered:

- CPU type and clock speed;
- Amount of RAM;
- Amount of persistent storage;
- Operating system.

In case a multi-components device is used, the operating system must fully support all the connected sub-components (document reader, biometric capturing device, etc.).

External memory expansion cards or disks could be considered if the chosen architecture module does not foresee permanent online connection and consequently requires that data or biometric samples will be collected and stored on the device during a shift and uploaded on a server offline at the end of the day. SD and micro SD cards are becoming popular memory expansions for PDAs and smartphones. In this case, security measures should be adopted for this kind of storage as well.

Additional hardware characteristics or aspects should be taken into account:

Displays: for devices intended for outdoor used, the capability to display text and images in bright sunlight as well as in the dark must be considered.

Audio feedback: or equivalent vibrating could be important as an additional mechanism to provide feedback to the operator from the device.

Memory expansion capability: several options could be considered: USB ports, serial ports, PCMCIA slot, SD slot, etc.

Fingerprint capture device: hardware aspects related to fingerprint sensors which could be considered include:

- Use of a finger guide on the fingerprint sensor to optimise placement of the finger
- Auto capture of image vs. manual capture of image
- Use of membranes to improve the ability to capture dry fingers

Facial image capture device: for facial image acquisition, the most important hardware issue to be taken into account is related to illumination, in this case the need for high-quality flash as opposed to onboard illumination should be evaluated.

Textual data entry: assuming that textual data from the documents can be acquired by the device using some type of scanner (OCR, bar code reader, MRZ reader, magnetic stripe reader, etc.), the use of a textual data entry device might be limited. Based on this consideration, the decision to be taken is whether a virtual or a physical keyboard is preferred. The choice may also be dependent on environmental conditions. Some users have reported a difficulty in using virtual keyboards while wearing gloves which might be particularly relevant in low temperatures.

Power and autonomy: some requirements related to power and autonomy where already identified in the questionnaire in which a question related to autonomy was the only one to get 100% support. Other aspects which could be considered include: availability of hot swap batteries, possibility to charge from a variety of sources, indicators for battery life and battery charge.

4.4 Risk Evaluation

The NIST BPR documents identifies three risk levels, which represent three levels of risk to public safety which might result from failure to identify properly an individual. Each risk level is then associated to a SAP level which is considered appropriate to mitigate

that risk. The SAP level, in turn, as described in section 2, identifies the values for the parameters associated to the biometric samples taken and capture details.

The three levels are:

- Severe (loss of property or life if accurate identification or verification is not made)
- Moderate
- Mild

Based on the experience gathered so far from the member states, e-MOBIDIG should collect and analyse the information necessary to identify threats resulting from failure to identify or verify the identity of an individual, their likeliness to occur and their risk levels and map biometric and other security requirements on them (this should not be confused with the security threats and countermeasures on the mobile identification system which are mentioned in [17] and described in the next chapter of this report). Requirements could be further detailed considering the three basic biometrics function: enrolment, identification, in case different measures need to be taken.

Complex and articulated formal methodologies, including ISO standards, do exist for risk assessment. A simple approach to address mobile communication is presented in [27] which provides an overview of methodologies for qualitative risk assessment in mobile environments.

The basic idea is to use an evaluation matrix in which increasing values for **likelihood** are displayed on the x-axis while increasing values for **impact** are displayed on the y-axis. Likelihood can de defined in the scale: unlikely-likely with different levels of intermediate values, while impact can be defined, similarly to the NIST document with values in the scale: mild-severe. The risk can thus be classified as minor, major, critical according to the perceived or analysed values for likelihood and impact. Typically, a risk that is ranked as "minor" requires no additional countermeasures, a "major" one needs to be dealt with and a "critical" one must be addressed with the highest priority.

A similar matrix which calculates risk management as a function of impact and likelihood is also presented and discussed by the Integrated Risk Management Framework [28] (Figure 4). An alternative way of classifying risk in a distributed system environment is suggested in [28]. Here risk is classified based on the motivation factors that drive an attacker. In this case, the two variables that can be considered are the level of motivation vs. the difficulty in carrying out the attack which becomes a threat and hence a risk for the system. Introducing a classification of threats and vulnerabilities and consequent countermeasures is also at the basis for the security assurance definition in a Common Criteria Protection Profiles [Section 5.4].

While these might seem more appropriate to evaluate risk associated to the mobile device and its operating environment rather than to evaluate risk in the meaning associated to the NIST risk levels, these methodologies provide useful procedures which could be evaluated by e-MOBIDIG to perform risk evaluation taking into account its specific use cases.

Alternatively, other methodologies do exist and can be applied to evaluate risks associated to mobile identification environment (including Special Publication 800-30 from NIST). Independently of the methodology chosen, e-MOBIDIG could make an effort to define a pan-European identification and classification of the risks associated to the use of mobile identification devices, and provide a joint evaluation of likelihood, impacts and acceptable level of risk. Such an evaluation could be the basis for a homogeneous evaluation of available solutions. A detailed risk assessment could then be the basis for the systematic identification of threats and associated attack potentials which can be subsequently used to define the security objectives in a possible e-MOBIDIG protection profile to be defined under the Common Criteria scheme.

Figure 4: Risk management actions as a function of impact and likelihood [IRMF]

5 TESTING, EVALUATION AND INTEROPERABILITY

The availability of reference standards ensures that products and software produced by different vendors can respect the same standard requirements and characteristics and seamlessly work together. Standards prevent vendor lock-in, help system work together, simplify support for multiple technologies and form the basis for interoperability when data created on a system or on a device or in a country (such as biometrics identifiers) must be interpreted and recognised by other systems and devices in other countries.

Testing for conformity to standards is a process which ensures that implementations which claim conformance to a standard, effectively respect its requirements. Although conformity to standards is not in itself a guarantee for interoperability of products from different vendors, it is nevertheless an important step to ensure conformity and interoperability of devices.

The concept of interoperability itself is rather broad. It can be seen from different perspectives from syntactic to semantic to organisational aspects.

Examples of standards relevant for testing and certification of the components which constitute a mobile identification device are the following:

Biometrics

- Fingerprint scanner: IQS (PIV, IAFIS, BSI, SAP…)
- Matching algorithms (FAR, FRR): FVC2006

Electronic document reader

- ICAO 9303 layers 1-4 and 6-7
- ISO/IEC 7816, ISO/IEC 14443 A/B, ISO/IEC 10373

Environmental issues

- IP Code 40, 54, 65 (IEC 60529)
- MIL-STD-810F

In mobile identification the data exchange aspect is also important, i.e. the way that information is "packaged", what information is exchanged and how it is described

(syntax and semantics). An example of a syntax standard, i.e. how the data is formatted is XML, an example of a standard which defines the data to be transmitted in the case of biometrics records exchange is ANSI/NIST-ITL (which is also used by German BKA, for instance, in a German adaptation which is known as GSAT 2.1, German Standard for AFIS Transactions).

Regardless of the application domain – telecommunication, transportation, health care, computation, or etc – services are provided by distributed, interconnected systems composed of products from different vendors. These systems are highly modular and may be based on multiple technologies which evolve at different pace. The high level architecture presented in section 4.1 is an example of the heterogeneity of technologies. The effort for seamless integration is therefore continuous.

Interoperability is particularly important in the communications industry which is, by its own nature, borderless and for this reason the communication industry has a long history in developing standards and conformity testing. The European Telecommunications Standards Institute ESTI defines Conformity testing as "*the act of determining to what extent a single implementation conforms to the individual requirements of its base standard"*, while interoperability testing is *"the act of determining if end-to-end functionality between (at least) two communicating systems is as required by those systems' base standards"*[16].

As standards and conformance testing become more and more complex, bi-lateral testing and interoperability events, in which various vendors implementing the two sides of a communication service meet and test the interworking of their products, are increasingly accepted as a solution to improve interoperability, however they cannot guarantee that products follow standards correctly. In other words, two products may be able to interoperate even if they do not pass conformance tests while on the other hand, conformant products may still not interoperate in some circumstances. When two implementations don't interoperate, this may be due either to ambiguities or options in the standard specifications. Options or ambiguities can be interpreted by vendors in different ways. As a result, the two implementations might not exhibit the same behaviour in some circumstances. One example is the case of an error code reported by passport chips which can be used to fingerprint passports. Even interoperability test events in controlled environments do not necessarily guarantee interoperability on the field. This is particularly true if implementations tested in a controlled environment are allowed to change the systems behaviour during the test execution.

[16] www.etsi.org

The International Standards Organisation (ISO) defines Conformity Assessment (or Conformance Testing) as the *"activity that provides demonstration that specified requirements relating to a product, process, system, person or body are fulfilled"* and Interoperability as the *"ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively, and consistently, and to use the information that has been exchanged"*. Conformance enhances the chance of interoperability but doesn't necessarily guarantee it. On the other hand, interoperability is one of the key factors to success when deploying new technologies for highly distributed systems.

Interoperability is fundamental for worldwide usability of electronic passports, for this reason many interoperability test events have been held to test ICAO electronic passports, some of them were organised by ICAO. The last event, held in 2008 in Prague, was organised by the BIG and included interoperability testing for the Extended Access Control (EAC) protocol. One of the most complex aspects in testing interoperability for EAC is the PKI which is needed to handle the CVCA/DV certificates and the SPOC protocol which is used to exchange CVCA certificates between "EAC enabled" countries. In the Prague tests, test PKI were used to handle certification but SPOCs were not included.

5.1 Conformance testing for the documents reading functional module

The process of reading an electronic passport equipped with a contactless chip is a contactless transaction which occurs between a contactless reader, called a Proximity Coupling Device (PDC) and a contactless chip, called a Proximity Integrated Circuit Card (PICC). The protocol which defines the way they communicate is described in the international standard ISO/IEC 14443 which consists of four parts and covers two types of cards known as Type A and Type B, both used for passports. PICC and PDC communicate via radio at 13.56 Mhz at a distance range between 0 and 10 cm.

Conformity tests for the document reading component of the high level architecture outlined in this paper is defined in the case of electronic passports in [46] [47], [48] and in [11].

The three ICAO documents on RF Protocol and application test standard for e-passport [46], [47] and [48] define the test plans respectively for layers 1-4 (i.e. initialisation, anti-collision and transport), layers 6 and 7 (application protocol and logical data structure)

and for e-passport readers (proximity coupling devices, PCD, using the standard terminology).

The tests defined in these documents reference directly the relevant ISO standards, i.e. tests for the physical and electrical parameters according to ISO/IEC14443-1 and -2, and tests of the initialization and anti-collision and the transport protocol according to ISO/IEC14443-3 and -4. The set of tests defined in the international standard ISO/IEC 10373-6, Test Methods for Proximity Cards, allows producers to test compliance of the equipment to the ISO/IEC 14443 standard.

Tests are defined in depth in order to minimize the probability that an error or fault in either side of a radio communication remains undetected.

ISO/IEC 10373-6 also describes the test apparatus set-ups and equipment required to perform the tests specified and the environmental parameters (e.g. temperature, humidity, bit rate, etc.) to be applied to the integrated circuit (IC) chips under test.

They prescribe also the format and content of the final test report which must contain the number of successful evaluations versus the total number of evaluations for each sample and for each test. The test report must also include for each test its description, the information whether the result was a pass or a fail, and the date of the tests.

The sequence for the execution of the test is also prescribed. The standard recomments that tests with all samples are performed in the same order. If the layer tests are carried out separately or are carried out with different samples, additional tests will be necessary.

The specifications include also destructive tests (e.g. mechanical and electrical stress tests).

Examples of tests for the PICC (on the communication layers 1-4) include:

- test methods for the initialisation of PICC
- handling of anti-collision
- test methods for logical operation of the PICC
- PICC load modulation amplitude test
- Alternate magnetic field test
- Operating field strength test
- Communication stability test
- Frame delay time test

Examples of tests for the PCD (on the communication layers 1-4) include:

- Test methods for PCD type A and for PCD Type B
- Test methods for logical operation of PCD
- Continuous monitoring of packets sent by the PCD

On the upper layers (6 and 7) the specifications contains several test units, one for each object in the logical data structure, i.e. the 16 data groups, the EF.COM file and the security data object (EF.SOD).

Layer 6 and 7 tests can be executed directly on a regular e-passport and require that the passport is fully personalised, i.e. all the data in the logical data structure (LDS) must be present. The input data for the test (simulating messages from the reader) can be provided through an input file. The source of test data is specified in the test configuration document.

When layer 6 and 7 tests are executed, it is assumed that the lower layers (electrical interface and the underlying transport protocol) have been functionally tested.

The third document of the ICAO test documents set provides an appendix with a table which compares tests for e-passports and tests for the readers (PCD) indicating which sets are optional and mandatory in the two cases.

In addition to the ICAO test specifications, the BSI Technical Report TR-03105 [11] provides a more detailed set of documents for conformity tests of electronic ID documents which include also a general framework which allows modular addition of test components. The framework enables tests organisations to easily modify and update subcomponents if necessary. The BSI Technical Report consists of several parts which comprise also tests for the German eID card and electronic signature application:

- BSI TR-03105 Part 1.1 A framework for Official Electronic ID Document conformity tests, Version 1.04.1
- BSI TR-03105 Part 1.2 Component Specification RFID, Version 1.02.1
- BSI TR-03105 Part 2 Test Plan for ICAO compliant MRTD with Secure Contactless Integrated Circuit, Version 2.2
- BSI TR-03105 Part 3.1 Test plan for Application Protocol and Logical Data Structure, Version 1.1.1
- BSI TR-03105 Part 3.2 Test plan for eMRTDs with Advanced Security Mechanisms – EAC 1.11, Version 1.12
- BSI TR-03105 Part 3.3 Test plan for eID-Cards with Advanced Security Mechanisms EAC 2.0, Version 1.03
- BSI TR-03105 Part 3.4 Test plan for eID-cards with eSign-application acc. to BSI TR-03117

- BSI TR-03105 Part 4 Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4 Version 2.2
- BSI TR-03105 Part 5.1 Test plan for ICAO compliant Inspection Systems with EAC, Version 1.2
- BSI TR-03105 Part 5.2 Test plan for eID and eSign compliant eCard reader systems with EAC 2; Version 1.1

Part 1.1, the framework document defines the standard test configurations and protocol formats, so that test scenarios for different modules can be integrated to a consistent assessment procedure. This allows existing test specifications to be easily integrated and scenarios for new components to be added as needed.

Figure 1 shows the overall framework defined in [11].

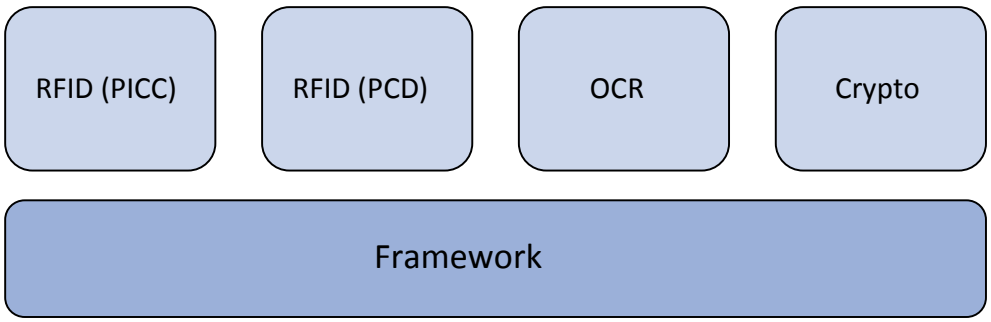

Figure 5: Test framework

The structure of the test components as defined in [11] recommends that all test components have the same structure except in those cases in which another, well known and used standard is defined, this is the case for instance of ISO/IEC 10373 and ISO/IEC 14443 for which the structure defined in the ISO document is used The test component in the case of ISO/IEC 10373 and ISO/IEC 14443 is defined as a list of:

- **Test description**: provides a short overview about the test scenario and describes the goals of the test.
- **Conditions**: states conditions that have to be accomplished in order to be able to start the test.

- **Parameters**: specifies the different kind of parameters that are needed to start the test case.
- **Report**: indicates the items that must be included in the test report, representing the final results of the tests executed.

The test framework defined in [11] consists of several test components combined in a modular way. A component encapsulates a well-defined area of the Official Electronic ID Document environment and has the following information:

- **Purpose**: defines clearly the area covered by the test component
- **Precondition**: Specifies the general requirements the test facility must meet to be able to perform the tests.
- **Importance**: indicates whether the area covered by the component is optional or mandatory
- **Layer specification:** indicates which layers are affected and which test procedures are used.
- The test components identified in the case of electronic passports (as shown in figure 5) are:
- **RFID (SCIC)** defining tests for the transmission and storage of the electronic data stored in the ePassports chip, covering only the covers the chip side.
- **RFID (PCD)** defining tests regarding the RFID reading device (PCD) including physical tests of the reader's electro magnetic field and the low level transmission protocol.
- **OCR** including the device capabilities of detection certain passport security feature and optical recognition of the machine readable data.
- **Crypto** including the crypto interface necessary to support the passport secure functionality.

So far no tests have been specified for the OCR and Crypto components in the framework of the BSI TR 03105 document.

Table 6 below shows the reference standard, per OSI layers, for RFID (SCIC), i.e. the passport and RFID (PCD), i.e. the inspection system.

Table 6: reference standard, per OSI layers, for RFID (SCIC) and RFID (PCD)

OSI Reference Layer	Layer description	Example of tests in this layer	Standard specifications
7 – Application	MRTD – LDS tests, including BAC and EAC	This layer contains several test units, one for each LDS object (DG 1 - 16, EF.Com and EF.SoD). Another test unit verifies the integrity and consistency of the different data structures.	ICAO Document 9303, BSI Technical Guidelines TR-03110
6 – Presentation	Smartcard – security and command tests	Commands such as: • Select LDS Application • Select File (FileID) • ReadBinary (B0/B1 with/without SFI) • Mutual Authenticate (For BAC support) • Internal Authenticate (For AA support) Are tested	ISO 7816, ICAO specs
5 – Session	-		-
4 – Transport	Proximity card transmission protocol	• Response for valid and invalid block formats • Response for valid and invalid block sequences e.g. chaining, re-transmission, frame waiting time, etc.	ISO 14443-4, ISO 10373-6
3 – Network	Proximity card initialisation protocol		ISO 14443-4, ISO 10373-6
2 – Link 1 – Physical	Proximity card hardware	Checks the behaviour of the card IC in relation to electrostatic discharge (ESD) exposure of the test sample.	ISO 14443 1-2, ISO 10373-6

Another important concept in the description of a test component is the test case, which covers a single test procedure. A test specification document is in fact a set of test cases. The test specification documents specifies which test cases must pass or can optionally be skipped for the implementation under test to be considered conformant to the specifications.

BSI TR-03105 Part 5.1 Test plan for ICAO compliant Inspection Systems with EAC [20] includes also test specifications specifically developed to test ICAO compliant inspection systems which implement extended access control. These specifications could be used as a starting point in testing the document reading component of mobile identification for what concerns conformance to the ICAO electronic passports specifications.

This document proposes a test plan to verify that the application component of the inspection system, which implements the ICAO passport reading functionality, is conformant to the ICAO (plus EAC) specifications.

This test plan consists of two separate parts. Layer 6 defines tests for the application protocol based on ISO 7816 requests (commands) issued by the inspection system application and the correct processing of the corresponding passport responses. Layer 7 verifies the correct processing of the logical data structure and content files read from the ePassport.

In order to define tests for inspections systems capable of reading both BAC-only and BAC+EAC passports, the specifications define two inspection procedures that an inspection system must support: a **standard inspection procedure** (BAC) and an **advanced inspection procedure** (EAC).

The test cases are formulated in such a way that they are independent of any specific system design or implementation.

The device under test is an inspection system (IS) that is used to read electronic passports optically and electronically. In a test setting, the inspection system reads the information contained in the electronic passport, displays the information to the user via a (graphical) user interface, provides biometric information to a biometric verification application and provides biographical information to other applications for further processing, such as backend databases, blacklists etc. An inspection system may contain different functional modules in addition to those purely dedicated to the reading of the electronic document. Such modules may for instance be dedicated to accessing the PKI and managing certificates, or accessing central databases, or processing data input and displaying user interface, etc. Only modules which read the electronic passports according to the [4] and [19] specifications are tested for conformity according to these test specifications. The remaining modules are not standardised and cannot be subject to conformance testing.

The inspection system under test must provide the following capabilities:

- A contactless reader interface according to ISO 14443.

- An optical interface to read the machine readable zone (MRZ) from the electronic passports data page (or alternatively, a keyboard device should be provided to enter the MRZ manually).
- A user interface which is capable of signalling to its user that some information has been retrieved from the electronic passport (layer 6 tests) and that this information is correctly formatted and authentic (layer 7 tests).
- A logging file, which can be used by the test engineer to investigate the tests results in a deeper way.
- An interface to upload certificates for passive authentication and for terminal authentication:
    - Terminal authentication test keys (IS private key)
    - Test certificate chains for terminal authentication
    - Test certificate chains for passive authentication

  Certificates must be available for the tests, however, testing the PKI or the interface to obtain and manage certificates is not specified in any standard, it is implementation dependent and although it is fundamental in order to be able to perform all tests which involve cryptography, testing PKI functions is outside the scope of any testing for conformity.

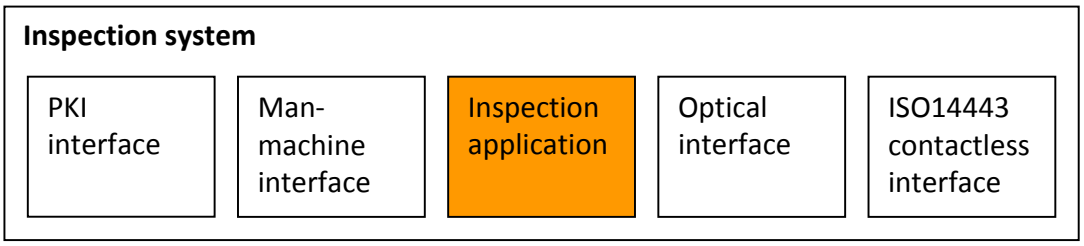

Figure 6: Functional components of an inspection system[17]

Outside of the scope of the tests specified in [11] are also the optical reader or scanner and optical inspection of the security features of the electronic passport.

As already mentioned in the discussion about the ICAO Guide [49], the inspection system must be able to support all the algorithms which can be implemented in the electronic passport in order for it to be able to read and interoperate with any standard

[17] From [10]

conforming passport. Passports, on the other hand, may implement only a subset of the algorithms and protocols specified in the standard.

There exist on the market products which implement the complete test suites described in the standards both for the communication layers (1-4, ISO/IEC 10373-6) and for the application layers (6-7, logical data structure and security). Often they are offered together with the necessary test apparatus. When chips (PICC) are being tested, the reader can be emulated by test apparatus able to simulate all the test conditions described in the test cases. Vice-versa, when readers (inspection systems) are being tested, the chip can be emulated by test apparatus able to simulate all the test conditions described in the test cases.

This extensive description of the testing environment and requirements for testing the conformity of an inspection system application for one type of electronic document was provided to give an idea of the operations required to test the document reading capabilities of a mobile identification device. The inspection system application is at the core of document reading software component for a mobile identification device as well as for stationary system. Similar types of tests, test environment, component and considerations apply to any other standard document which should be read and processed by the mobile identification device. This is particularly true of the electronic documents for which interoperability between different countries would be a desirable feature.

5.2 Conformance testing for the biometrics functional module

The definition of coherent quality requirements for different biometric applications (ePassport, VISA, ERP), covering all biometric functions: enrolment, verification, identification, is an important step in guaranteeing:

- Interoperability, modularity, reusability, extensibility
- Clear software architecture with well-defined interfaces
- Establishment of certification procedures for conformity assessment

Also for biometrics, there are some standards defined for a framework and corresponding test conformance that is defined by the German BSI. The set of documents and their scope have been presented to MOBIDIG in one of the first workshops. The whole set of documents, which is available from the BSI website, comprises:

- BSI TR-03121-1 Technical Guideline Biometrics for Public Sector Applications. Part 1: Framework, Version 2.3
- BSI TR-03121-2 Technical Guideline Biometrics for Public Sector Applications. Part 2: Software Architecture and Application Profiles, Version 2.3
- BSI TR-03122-1 Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 1: Framework, Version 2.3
- BSI TR-03122-2 Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 2: Software Architecture – BioAPI Conformance Testing, Version 2.3
- BSI TR-03122-3 Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 3: Test Cases for Function Modules, Version 2.3

The framework provides a common architecture which allows consistent comparison of the quality of biometrics components.

It defines standardised quality requirements for various kinds of biometric applications in the public sector, standardised security requirements and modular software architecture. Existing standards, in particular ISO, are taken into account.

The following components are considered in the framework architecture:

Acquisition Hardware: Devices that are used for digitising physical represent able biometric characteristics (e.g. fingerprint scanners, digital cameras, signature tablets, etc.).

Acquisition Software: interface software (drivers) between the acquisition hardware and the image processing software.

Biometric Image Processing: provides the extraction of all relevant biometric information from the image.

Quality Assurance: checks the quality of the biometric data.

Compression: compresses the biometric data losing too much quality for a biometric verification or identification.

Coding: formats quality data as well as biometric data in defined formats, which can be required for data interchange. The use of standard formats (such as ANSI-NIST-500-271) facilitates interoperability.

Biometric Comparison: encloses the mechanisms and algorithms to verify or identify an identity based on a one-to-one or one-to-many biometric comparison

between reference data (stored in a document or in a database) and a captured biometric sample (usually a live presented image).

The framework architecture is based on the BioAPI 2.0 specifications. BioAPI (Biometric Application Programming Interface) is the standard ISO/IEC 19784-1, produced by the ISO/IEC Joint Technical Committee 1 (JTC1), Subcommittee SC37 Biometrics. The purpose of the standard is to define an architecture and all necessary interfaces to allow biometric applications (optionally distributed across a network) to be integrated from modules provided by different vendors.

The BioAPI architecture, as shown in **Error! Reference source not found.**, is structured in the following components:

- The **biometric application** uses biometric functionalities for a defined purpose, e.g. the acquisition of biometric data to be checked against the images stored in electronic identity documents or the acquisition and verification of biometric data for access control.
- The **BioAPI framework** provides the required biometric functions to the application.
- A **Biometric Service Provider (BSP)** which implements a biometric functionality that is loaded and administrated by the framework. The framework can load several BSPs and provide their functionality to the application.

In 2007 the international standard ISO/IEC 24709:2007 for conformance testing of BioAPI components was published. The standard defines the necessary methods, procedures and test assertions to check conformance to the base BioAPI standard, for all different kinds of components of the architecture model that are used.

The ISO/IEC 24709:2007 consists of three parts:

- Part 1 of the standard [ISO/IEC 24709-1:2007] describes the general procedure for the conformance testing. It provides guidelines for specifying BioAPI conformance test suites, for writing test assertions and defining procedures to be followed during the conformance testing are provided. The conformance testing methodology is concerned with conformance testing of biometric products claiming conformance to BioAPI. Definitions of schemas of the assertion language in XML are provided in normative annexes.
- Part 2 of the standard [ISO/IEC 24709-2:2007] contains the test assertions that have to be performed for conformance testing of the BSPs. The test cases are defined in a XML based language, which is specified in ISO/IEC 24709-1. These assertions enable a user of ISO/IEC 24709-2:2007 (such as a testing laboratory)

to test the conformance to ISO/IEC 19784-1 (BioAPI 2.0) of any biometric service provider (BSP) that claims to be a conforming implementation of that International Standard. Assertions are placed into packages (one or more assertions per package) as required by the assertion language.

- Part 3 of the standard [ISO/IEC 24709-3:2011] defines a number of test assertions written in the assertion language specified in ISO/IEC 24709-1:2007 to test the conformance to ISO/IEC 19784-1 (BioAPI 2.0) of any BioAPI Framework that claims to be a conforming implementation of ISO/IEC 19784-1.

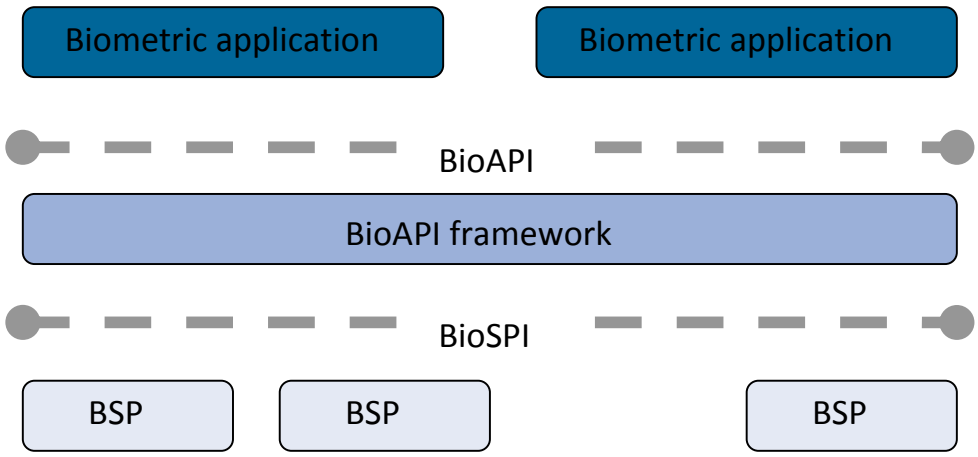

Figure 7: BioAPI framework [5]

Conformance to the BioAPI specifications should ensure that systems produced by system integrators using components from multiple vendors are capable of interoperating correctly.

The Conformance Test Specifications for the biometrics application consists of three parts:

- The framework which introduces the structure of the Conformance Test Specification, describes the need for the Conformance Test Interfaces and gives an overview about the conformance instruments
- The BioAPI architectural model which explains the layer-structured tests and the test methodology.

- The test cases for conformity to the functional modules.

In order to obtain certification for conformity to the BioAPI specifications, the following conformance instruments are used:

> **Conformance test tools:** software components that are used to check the compliance of the BSP by comparing the expected result with the actually received result.
>
> **Appropriate conformance test databases**: specific test data that are used by the evaluation laboratory to perform certain test cases.

An example of a test case specified in the framework of the BioAPI conformance testing (adapted from [9]) is the following:

> ***Test case***: Examination of automatic acquisition of the fingerprint image
>
> ***Preconditions***:
>
> - A single fingerprint sensor is connected
> - The module (Fingerprint Enrolment BSP) is loaded and a session is attached
> - As necessary test resources: finger of a test person
>
> ***Test execution***:
>
> 1. Start of the acquisition and correct placement of the finger on the sensor
>
> Expected result: The activation of the acquisition occurs automatically at the latest at the end of the time-out.
>
> 2 Start of the acquisition without placement of a finger on the sensor
>
> ***Expected result***: An adequate error message is given that no fingerprint has been captured successfully.

NIST also offers an implementation of the Conformance Test Suite for BioAPI 2.0, which can be downloaded from http://www.nist.gov/itl/csd/biometrics/bioapicts.cfm.

Testing quality of the main biometric components

The main biometric function that should be supported by a mobile-ID device are verification 1:1 and identification 1:N. The enrolment of biometric data in mobility is required mainly for military use.

In all cases it is important to capture high quality images, even if with different degrees, higher quality for the identification and lower quality for verification.

If recognition is made locally the accuracy of recognition is related to the biometric data quality and the quality of comparison software running on the device; for identification software with high accuracy and speed of matching is required; for 1:1 verification the comparison software can be of lower quality.

If recognition occurs in a remote database (central national AFIS or in the European VIS/BMS) the recognition software is placed in the central system; usually the software in a central system is a high performance in terms of both accuracy and speed.

In these cases mobile devices must acquire images with quality and features required by the central systems, most notably resolution and size, and images must be properly compressed and formatted according to the format prescribed by the central system for transmission.

For example, the captured biometric data to be sent to the VIS/BMS is compressed and coded according to the VIS-ANSI/NIST specification [34].Note that the biometric comparison is done by the VIS BMS.

Conformance testing of fingerprint acquisition device

Acquisition is a critical step in determining the quality of the fingerprints that are used for local or remote verification.

The factors below can affect the quality of the capture:

- device quality
- acquisition method and capture operator's knowledge
- subject's experience about fingerprint capture
- acquisition environment (light, temperature, quality of fingers etc)

There are a few standards currently in use in order to define the image quality requirements for fingerprints scanners:

- **The IAFIS Image quality specifications** (IQS), defined in Appendix F of the Electronic Biometric Transmission Specification (EBTS) [35], has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large scale machine many-to-many matching operation.
- **PIV-071006 [37]** is a lower-level standard designed to support one-to-one fingerprint verification, established by the US Federal Bureau of Investigation (FBI) for the US

Personal Identification Verification program, whose aim is to improve the identification and authentication for access to U.S. Federal facilities and information systems. Certification is available for devices intended for use in the FIPS 201 PIV program.

- **PassDEÜV**: established by the German Federal Office for Information Technology Security (BSI) for the capture and quality assurance of fingerprints by the passport authorities and the transmission of passport application data to the passport manufacturers [38]; the PassDEÜV requirements are identical to the FBI AFIS requirements except for the acquisition area, which can be smaller (16 x 20 mm). List of products certified according to BSI Technical Guidelines are published on the BSI internet pages.

Since mobile devices may satisfy a variety of collection modalities with differing image size and accuracy requirements, NIST defined a set of subject acquisition profiles for fingerprint images, labelled 10-60. Table 3: NIST SAP levels and related standards in Chapter 2 summarizes the image sizes and IQS specification relevant for each image interchange profile. More information on the profiles and best practices associated with mobile ID systems can be found in [1].

Mobile ID devices can operate in a mobile environment. Only flat impressions are required. The category is sub-divided into several levels by subject acquisition profile (SAP) number, based upon device capture dimensions, the image quality specification applied, and the number of simultaneous fingers that can be captured.

When the IQS specification requirement is IAFIS-App F, then all requirements of [35] shall be met. When the IQS specification requirement is PIV, then all the requirements in [37] shall be met.

SAPs 10, 20 and 30 are for single finger sensors with SAP 10 having the same minimum image dimensions as the Federal Information Processing Standard (FIPS) 201.

SAPs 40 and above support simultaneous capture which is faster, reduces sequence errors and produces higher quality images.

As detailed in [1] an agency will select a SAP based on their specific requirements.

Level 20 is the minimum SAP level recommended by NIST for fingerprint verification in severe risks environment.

According to [34] VIS/BMS is expecting fingerprint images of 400 (HLL) by 500 (VLL). Other fingerprint image sizes are also allowed and accepted, however individual fingerprint images should not be bigger than 512 x 512. These indications suggest, for biometric checks in the VIS/BMS, the use of SAP level 30 capture device (image size 400 x 500 ppi).

In pilot projects carried out by member states to verify e-MRTD documents, presented in the e-MOBIDIG meetings, capture devices ranging from SAP level 10 to SAP level 30 have been used.

Regardless of the SAP level chosen, it is recommended that the fingerprint capture device is certified by an independent test laboratory or an official agency.

A white list of mobile capture devices certified by FBI is available at https://www.fbibiospecs.org/IAFIS/Default.aspx. As of 07/10/2011 there are 27 mobile single/dual finger capture devices in the FBI list ranging from SAP level 10 to SAP level 45.

Test procedures to verify compliance of fingerprint scanners to IAFIS IQS can be found in [39].

Test procedures to verify compliance of fingerprint scanners to PIV IQS can be found in [40].

According to the test procedures, verification of compliance of a scanner to the full set of IAFIS or PIV IQS requirements is primarily performed by verification through systematic exercising of the capture device with sufficient instrumentation to show compliance with the specified quantitative criteria. A few requirements are verified by visual examination of the item or review of descriptive documentation.

The main parameters characterising the acquisition of a digital fingerprint image verified during the test are as follows:

- **Area**: size of the area sensed by the fingerprint scanner.
- **Geometric accuracy**: determined by the maximum geometric distortion introduced by the acquisition device.
- **Resolution**: denotes the number of dots or pixels per inch (dpi)
- **Signal-to-noise ratio** (SNR): quantifies the magnitude of the noise with respect to magnitude of the signal.
- **Spatial frequency response**: denotes the ability to transfer the details of the original pattern to the output image for different frequencies and is usually measured through Modulation Transfer Function (MTF)
- **Gray range**: is the actual number of gray-levels used in the output image (e.g., 8 bits per pixel yields 256 level of gray).
- **Gray level uniformity and input-output linearity**: the gray level uniformity is defined as the gray-level homogeneity measured in the image obtained by scanning a uniform gray patch; the input-output linearity quantifies the deviation

of the gray levels from a linear mapping when the input pattern is transformed into an output image.

Following is a listing of the commonly used scanner test targets:

- Multiple parallel bar target at 1.0 cycles per millimetre (cy/mm) for *geometric accuracy* and *pixels per inch resolution* tests.
- Sine wave target with gray patches for Modulation Transfer Function (MTF) and linearity tests.
- Uniform dark gray and light gray targets for signal-to-noise ratio and gray-level uniformity.

Scanner testing also includes scanning a set of fingerprints.

Test data analysis software (freeware) is available through the FBI.

Performance evaluation of biometric recognition algorithms

Performance evaluation of matching systems is defined by a fingerprint database and an associated testing protocol.

Since June of 2003, NIST has been conducting evaluations of fingerprint-based biometric matching systems using vendor supplied SDKs and fingerprint databases [41], [42].

Fingerprint Verification Competitions (FVC) were organized in 2000, 2002, 2004 and 2006 by Biometric Systems Lab University of Bologna, Pattern Recognition and Image Processing Laboratory, Michigan State University, Biometric Test Centre San Jose State University [40] using databases of different size and difficulty. The difficulty of each database depends on several factors: population, scanner quality, acquisition process, etc.

To make test results more predictive of real world performance, testing standards are being developed (ISO/IEC 19795) [44].

FVC data collection and protocol comply with the above cited standard.

Fingerprint verification consists in comparing two fingerprints to determine whether they are impressions of the same finger or not (one-to-one comparisons).

During performance evaluation, genuine (matching two fingerprints of the same finger) and impostor (matching two fingerprints originating from different fingers) attempts are performed to compute False Non Match Rate FNMR (also referred as False Rejection Rate - FRR) and False Match Rate FMR (also referred as False Acceptance Rate - FAR).

Performance against the database will depend upon both the environment and the population in which it is collected. Consequently, quality of fingerprints in the database should be consistent with the quality of data recorded in the documents to be checked.

The size of dataset will affect how accurately we can measure error rates. The larger the dataset, the more accurate the results are likely to be.

FVC-onGoing is the evolution of FVC; is a web-based automated evaluation system for fingerprint recognition algorithms. Tests are carried out on a set of datasets and results are reported on-line by using well known performance indicators and metrics. The results do not necessarily reflect the performance that the algorithms would achieve in a real environment or when embedded into a complete biometric system but give a useful overview of the state-of-the-art in this field.

According to recent results published on FVC web site, the average FRR of the three most accurate algorithms, at a FAR of 0.1 %, is about 0.13%. These results, obtained with the standard database containing fingerprint images acquired in operational conditions using high-quality optical scanners, should reflect the expected accuracy in large-scale fingerprint-based applications as e-passport and e-residence permit card, using high quality fingerprint scanners and the best matching algorithms.

It is recommended that the achievable performance of the fingerprint matching algorithm used for local verification or identification is measured by an independent test laboratory or an official agency. The operating agency should not rely on performance figures given by the algorithm provider only.

According to the results of test pilot carried out by a MS with SAP 10 devices and first class matching algorithms, presented in the 4th MOBIDIG workshop, the FRR was 0.0025 (0.25%) at a FAR of 0.001 (0.1%) in 1:1 biometric verification on tablet pc.

The performance of matching algorithms on devices with less processing power and slower memory, such as PDAs and smartphones or add-ons, could be significantly lower, with the same verification time, compared to the performance obtained on standard PCs.

5.3 Conformance testing for the data communication functional module

Conformance testing for data communication links is generally conducted in the framework of the certification of the communication component of a device. Standards

in this sense are defined by standards organisations such as ETSI and should not be a concern for service users such as the mobile identification application would be.

5.4 Security evaluation and the Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC), which has recently been adopted by ISO as a full international standard (ISO/IEC 15408) [52], [53], and [54], is a standard used in the information and communication technology industry to ensure that products can be evaluated by independent and accredited licensed laboratories in order to determine the fulfilment of particular security properties, to a certain extent or assurance level.

The Common Criteria standard consists of three parts: Part 1 contains the descriprion of the general model, Part 2 contains a catalogue of functional security requirements, Part 3 is a catalogue of security assurance requirements. This structure providess great flexibility in the specification of secure products. Common Criteria functional requirements and assurance requirements components can be collated by interested user communities such as consumers, national security authorities, government users, commercial users, system integrators, platform developers, etc. to specify the security functionalities required for a product to meet their security needs. Such selections constitute Protection Profiles or Security Targets. More precisely a ***Protection Profile (PP)*** is an implementation independent security specification for a category of products. It consists of a list of functional requirements, a list of assurance activities and justifications that they address the threats that the product has to withstand. PPs can themselves be considered as international standards.

Security Targets (ST) on the other hand contains the security objectives and requirements of a specifically identified product (as opposed to a class of products) and defines the functional and assurance measures offered by that product to meet stated requirements. The ST may claim conformance to one or more PPs.

The Common Criteria are the result of the combination of a large number of national standards dated back to the early 1980's, the most important being the TCSEC approach practised in USA and the ITSEC approach practised in Europe, both initially developed to certify the security of operating systems.

The list of assurance activities (EAL, Evaluation Assurance Level) concept, which range from EAL1 to EAL7 in the Common Criteria, is an inheritance of the ITSEC specifications.

Evaluation assurance covers many aspects of the product lifecycle from development to vulnerability assessment through requirement analysis, guidance documents, testing,

etc. These classes of assurance activities address systematically, with increased level of depth, all failings in which an IT product can become vulnerable (e.g. failings in requirements in implementation, in operation, etc.) and form the content of the EALs.

Table 7: ISO/IEC 15408 EAL levels

EAL1	Functionally tested	Limited security target, evaluation is conducted without assistance from the developer of the product.
EAL2	Structurally tested	Requires delivery of design information from the developer. The level of independently assured security is low.
EAL3	Methodically tested and checked	Requires a thorough investigation of the product and its development without substantial re-engineering.
EAL4	Methodically designed, tested and reviewed	Provides a moderate to high level of independently assured security. May require additional security-specific engineering costs.
EAL5	Semi-formally designed and tested	Provides a high level of independently assured security. Requires rigorous development approach without requiring costs associated to additional specialist security engineering techniques.
EAL6	Semi-formally verified designed and tested	Requires additional costs and is suitable to application in high risk situations where the value of the protected assets justifies the additional costs.
EAL7	Formally verified designed and tested	Applicable to products with tightly focused security functionality that is amenable to extensive formal analysis.

Vulnerability assessment is a particularly important assurance class as it is aimed at assessing, through penetration testing, the resistance against attack potential.

Penetration testing addresses all the claimed security functions, threats identified and aimed vulnerability assessment level in the protection profile

Attack potential is a concept defined in the Common Criteria Methodology (CEM) [55], representing the difficulty of carrying out a successful attack. CEM defines also the method for calculating the attack potential, which is based on the evaluation of:

- Elapsed time (0-19 points)
- Specialist expertise (0-8 points)
- Knowledge of the product being evaluated (0-11 points)
- Window of opportunity (0-10 points)

- IT hardware/software or other equipment (0-9 points)

An attack potential is basic if all attacks require at least 10 points, a high potential attack requires at least 25 points.

A concept that could be interesting for e-MOBIDIG is the concept of the Protection Profile (PP) which the group could define in order to provide a standard way to assess the security of mobile identification devices.

The specification of a protection profiles must contain the following sections:

Introduction: contains the identification and abstract of the protection profiles

Security Objectives: contains the stated intent to counter identified threats. Security objectives are defined in terms of threats, policies and assumptions on the environment.

TOE description: contains a description of the Target Of Evaluation (TOE), i.e. the class of products which is the subject of the PP and provides the content for the evaluation

IT security requirements: contains the list of functional and assurance requirements from the catalogues contained in parts 2 and 3 of the standard which a compliant TOE must address.

TOE security environment: contains a narrative statement of the security problem to be solved by the TOE. Describes the security aspects of the environment in which the TOE is intended to be used. This section addresses all assumptions including physical, personnel and connectivity aspects of the environment as well as organisational security policies that the TOE must be compliant with.

While the formal definition of a PP is a complex task which requires knowledge of the security functions and assurance from the CC catalogue, an important starting point that the e-MOBIDIG group could focus on is the identification of the threats, attack potentials and countermeasures, as well as the security requirements on the environment which can then be used to identify the proper function classes in the CC which should be referenced in the PP.

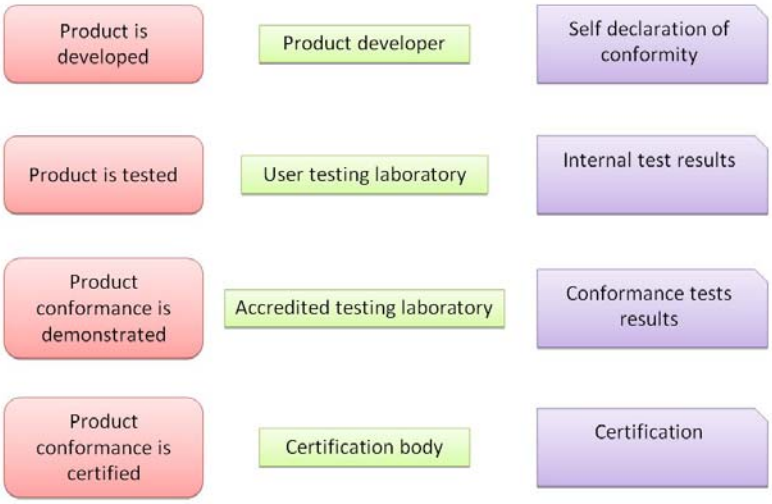

Figure 8: Steps to certification

5.4.1 Relevant protection profiles

The Common Criteria Portal (http://www.commoncriteriaportal.org/) contains a list of the protection profiles which have been defined under the Common Criteria specifications and the list of devices, equipment or software which has been evaluated and certified against such protection profiles specifications. These specifications can be used by vendors to have their products certified and can be referenced by newly defined PPs which are related to TOEs which use the TOEs in these PPs as (part of) their components.

The portal distributes the protection profiles published so far in the following areas:

- **Access control devices and systems**: which contains protection profiles for the security evaluation of firewalls, intrusion detection systems and the U.S. Government Protection Profile Authorization Server for Basic Robustness Environments,
- **Biometric systems and devices**: which contains protection profiles for Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies , and Biometric Verification Mechanisms Protection Profile
- **Boundary protection devices and systems**: which contains several protection profiles related to personal firewalls
- **Data protection**: which contains protection profiles on cryptographic modules
- **Databases**: which contains protection profiles on database management systems

- **Detection devices and systems**: which contain several protection profiles on intrusion detection systems scanners and analysers
- **ICs, smartcards and smartcard related devices and systems**: which is the richest set and includes protection profiles on JavaCard, electronic residence permits, electronic passports, MRTDs, security module cards and health cards
- **Key management systems**: which includes U.S. Government Family of Protection Profiles for Public Key Enabled Applications for Basic Robustness Environments
- **Network and network related devices and systems**: which contains protection profiles on web servers, VPN and US security requirements for network devices
- **Operating systems**: which contains protection profiles for operating systems in networked environments
- **Other devices and systems**: which contains protection profiles for everything else which does not fit in the other categories such as voting machines, hardcopy devices, ATM, etc.
- **Products for digital signatures**: which contains protection profiles for crypto modules and digital signature creation devices.
- **Trusted computing**: which contains one protection profiles for trusted computing

The **ICs, smartcards and smartcard related devices and systems**, as well as **biometric systems and devices** contain set of PPs that could be relevant for e-MOBIDIG. The first section, in particular, contains a considerable number of PPs related to electronic documents and passports. Since PPs have a modular structure, in that they can include and ask for compliance to another PP, in the framework of working on a MOBIDIG protection profile for identification devices, it would be advisable to assess the currently existing PPs and, taking a modular approach, identify gaps which should be filled-in in order to reach the level of formalising some kind of security evaluation for mobile identification devices.

6 OVERVIEW OF THE SOLUTIONS ON THE MARKET PRESENTED TO E-MOBIDIG

In the eight MOBIDIG meeting from November 2008 to September 2011 representatives from EU-MSs for border control and law enforcement presented experiences based upon initial trials and the solutions adopted.

Starting from the sixth meeting, the e-MOBIDIG invited companies providing mobile ID devices for police or immigration to participate in its meetings. The aim was to establish a dialogue with industry, to increase mutual understanding and to explore possible ways in which industry and EU Member States could work more effectively together.

In this chapter the solutions presented in the meetings are classified and analyzed.

With the exception of few solutions aimed only at the biometric verification or identification, that will not be analysed, the solutions considered here enable to:

- Read and verify the authenticity of the documents (at least e-passport) using security features (BAC, AA, TA, EAC) and the identity of the individual using biometric verification 1:1,
- Carry biometric identification 1:n locally or remotely (AFIS or VIS with back end access)
- Access databases and remote back-end systems.

With reference to the four logical macro blocks described in Chapter 4:

- document reader;
- biometric capturing and matching;
- computing platform, application engine and user interface;
- secure data communication platform

these are all found in the solutions oriented to control of documents. The macro block to read the documents may be absent in solutions oriented to biometric identification.

From a hardware point of view, these components can either be integrated in one single device or consist of independent components which communicate with each other either via short-range radio communication (e.g. Bluetooth) or via wired connection. The choice of the particular hardware solution will be dependent on the application scenarios in which the device(s) will be used and on physical constraints such as:

- total weight of the device/devices;
- usability;
- flexibility;
- total cost;
- availability of existing legacy computing and communication devices (such as patrol car mounted computing & communication platform, PDAs, etc.).

According to Eurosmart[18] [56] we can define the following classes:

1) **Integrated device** : all the 4 macro blocks are integrated in the same device;
2) **Compact device (PDA/smartphone) with N-in-1 add-on reader**: a biometric and document reader is physically attached to a specific PDA or smartphone;
3) **Tablet PC with N-in-1 add-on reader**: a biometric and document reader is physically attached to a specific tablet pc;
4) **Mobile ID box**: document and fingerprint reader in one device to be connected by Bluetooth to portable computing and communication platforms as tablet PCs, PDAs and smartphones;
5) **Mobile biometric ID device**: biometric reader to be connected to PDA, smartphone or tablet pc.

Solutions in classes 2-3-4-5 use existing devices for computing and communication functionalities and this could be more cost effective than integrated devices. They are certainly the most appropriate choice if the operators or the patrol cars are already equipped with suitable devices.

Separating parts of the solution like in class 2-3-4-5 may make it easier to upgrade one part in isolation from the other or allow attachment to different options. Solutions in class 4 and 5, based on separated devices, are the most flexible but requires two or three devices instead of just one. In the fourth meeting the border guard of a MS presented their solution based on three devices: ultra mobile tablet pc with 2 devices (e-document reader and fingerprint reader) connected simultaneously by Bluetooth.

The following describes the main features of each class of solution.

[18] EUROSMART is an international non-profit association created in 1995 that represents companies, associations, laboratories and independent experts of the Smart-Security Industry for multisector applications

1 Integrated device

- Full eDocument & Biometric capability
- Contact and Contactless Readers
- MRZ reading with swipe reader or Camera
- Fingerprint reader: in most cases capacitive, size 12,8x18 mm (SAP 10) and more rarely optical with larger size (SAP 20 or more).
- Supporting full range of communication (USB, Bluetooth, Wifi, GSM/GPRS/EDGE)
- Weight: 550-800 gr.
- Display size: 3,5”-3,7”
- IP 54 (or 65) compliant
- Operative system: windows mobile, CE or other mobile OS

Some devices, equipped with full page optical scanner, have bigger size and weight > 1 Kg.

2. Compact device (PDA/smartphone) with 4-in-1[19] add-on reader

- eDocument & Biometric capability
- MRZ reading with swipe reader or Camera
- Add-on solution

Similar to class 1 in terms of weight, screen size, mobile OS (RIM, android, iOS, windows mobile, Linux)

3. Tablet PC with 4-in-1 add-on reader

- eDocument & Biometric capability
- MRZ reading with swipe reader
- Weight: 1400-2100 gr. (included add-on)
- Display size: 5.6”-8.4”

[19] 4-in-1 add-on incorporates a biometric fingerprint reader, contact and contactless card reader and MRZ reader; there are also 3-in-1 add-on (without smart card reader) and 5-in-1 or 6-in-1 add-on with barcode reader and magnetic stripe reader.

- IP 54 compliant
- Fingerprint reader: capacitive, size 12,8x18 mm (SAP 10), optical SAP 20
- Operative system: windows XP and Windows Vista, Linux

Pro: software portability from desktop, screen size, keyboard, performance (processor, RAM, etc.)

Con: weight, size

Some countries have chosen the smaller tablet PC (Ultra Mobile PC) as handheld device as they have the same operating system for desktop PCs allowing use of the same applications for document checks and biometric verification on both platforms.

The largest tablet PCs are usually installed in patrol cars.

4 Mobile ID box (document and fingerprint reader) connected by BT (or USB) to host device

- Compatible with existing portable processing platforms as tablet PCs, PDAs and smartphones
- eDocument & Biometric capability
- Require additional device (pc tablet or smartphone) to display the result and for back end access (connected by BT)
- Weight: about 500gr.

5 Mobile biometric ID device

- Biometric only, no document verification.
- Not fully equipped for document reading (no MRZ swipe, and some without contact or contactless reader)
- Face acquisition for enrolment with camera
- Fingerprint reader: capacitive SAP 10, optical SAP 20 or 30.
- Weight: 85-340 gr.

In many cases the analyzed solutions have certified biometric capture devices, but there is no evidence that the matching algorithm or the inspection system have been tested by independent laboratories. This is particularly critical for solutions with mobile

operating systems since for these operating systems it is more difficult to find certified software.

7 CONCLUSIONS AND RECOMMENDATIONS

The present document has provided an analysis of the technical, functional and interoperability requirements for a generic mobile identification solution.

The report starts from the findings and discussions held so far in the context of the e-MOBIDIG working group, defines a high-level abstract architecture for a mobile identification device, identifying its main components. It then analyses available standards, conformity tests for each of the components with a particular view to security and interoperability. Existing guidelines and recommendations from international organisations are also taken into account in the analysis and discussions.

From the analysis of the experiences and discussions in the e-MOBIDIG working group, it emerges that use cases and contexts are different and there is no "ideal solution" which fits all cases. At the same time, the market offers already numerous solutions which are able to accommodate the numerous scenarios that are conceivable in the context of identification and authentication using a mobile setting.

While the availability of many solutions is a guarantee for the adaptability to local requirements, settings or legacies, and is certainly positive, it is nevertheless of the utmost importance that accuracy in identity verification, document authentication and biometrics matching are comparable in order to avoid that results of these operations are different based on the different devices employed.

Devices used for mobile identification should be able to provide results to the same functionalities which have the same accuracy level and are thus comparable.

Presentation of the results of the various verification functions should also be provided in a standard way which does not give room to subjective interpretations.

Critical points that can be identified so far are:

- due to the unavailability of guidelines, solutions in place or in pilot use devices with different characteristics and performances for the same functionalities, which may result in differences in the resulting verification. Such differences may exist also with the results from the verification with stationary devices or with automated unmanned systems such as automated border control systems (or e-gates). A study in this sense with on the field data might provide useful information and data.
- as there are no general guidelines, there are no general certification requirements on the devices. Of course specific requirements can be established in setting up local pilots or solutions, but results again would not be comparable. Affected components would be not only the document reader, but also the

fingerprint scanner, the matching algorithm, their security level and protection against vulnearbilities, etc.

- the management of certificates required by the e-MRTD security functions is even more complex than it is in the stationary environment, particularly regarding the DV certificates required to perform the terminal authentication in the extended access control protocol which is required in order to check the fingerprints stored in second generation passports.

It is suggested that, based on the experience gathered so far, e-MOBIDIG should aim at drafting such guidelines, possibly identifying "high-level use cases" or use profiles, carrying out risk assessment, identifying parameters which apply to the profile, including or excluding issue such as, for instance, access to databases like SIS and VIS and suggest acceptable values or reference standards. Such guidelines could form the basis or provide elements for the definition of formal protection profiles which could then be used by industry to certify their products.

A further step might lead towards the organisation of test events in collaboration with industry, in which the interoperability of different solutions, compatible with the guidelines, can be assessed.

8 REFERENCES

[1] NIST, ***Mobile ID Device Best Practice Recommendation***, Version 1.0, July 2009, NIST Special Publication 500-280, http:// www.nist.gov/itl/iad/ig/upload/MobileID-BPRS-20090825-V100.pdf

[2] NIST ***Fingerprint image quality***, August 2004, NISTIR 7151

[3] NIST, ***Data Format for the Interchange of Fingerprint***, Facial and Other Biometric Information, NIST Special Publication 500-271, 2007

[4] ICAO Document 9303, ***Machine Readable Travel Documents***, Sixth Edition 2006, http://www2.icao.int/en/MRTD/Pages/Document9303.aspx

[5] BSI Technical Guideline TR-03121-1: ***Biometrics for Public Sector Applications*** - ***Part 1: Framework***, Version 2.3

[6] BSI Technical Guideline TR-03121-2: ***Biometrics for Public Sector Applications - Part 2: Software architecture and Application Profiles***, Version 2.3

[7] BSI Technical Guideline TR-03121-3: ***Biometrics for Public Sector Applications - Part 3: Function modules***, Version 2.3, BSI

[8] BSI Technical Guideline TR-03122-1: ***Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications*** - Part 1: Framework, Version 2.3

[9] BSI Technical Guideline TR-03122-1: ***Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications*** - Part 2: Software architecture and Application Profiles, Version 2.3

[10] BSI Technical Guideline TR-03122-1: ***Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications*** - Part 3: Function modules, Version 2.3

[11] BSI TR-03105 Part 1.1: ***A framework for Official Electronic ID Document conformity tests,*** Version 1.04.114.11.2008

[12] ISO/IEC 7816-4:2005, Ed. 2 ***Identification cards -- Integrated circuit cards*** -- Part 4: Organization, security and commands for interchange

[13] ISO/IEC 10373-6:2001, Ed. 1 ***Identification cards -- Test method***s -- Part 6: Proximity cards

[14] ISO/IEC 14443-1:2000, Ed. 1 ***Identification cards -- Contactless integrated circuit(s) cards*** -- Proximity cards -- Part 1: Physical characteristics

[15] ISO/IEC 14443-2:2001, Ed. 1 ***Identification cards -- Contactless integrated circuit(s) cards*** -- Proximity cards -- Part 2: Radio frequency power and signal interface

[16] ISO/IEC 14443-3:2001, Ed. 1 I***dentification cards -- Contactless integrated circuit(s) cards*** -- Proximity cards -- Part 3: Initialization and anti-collision

[17] JRC60747, ***Technical challenges for identification in mobile environments***, JRC Scientific and Technical Reports

[18] ISO/IEC 14443-4:2001, Ed. 1 ***Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards*** -- Part 4: Transmission protocol

[19] BSI Technical Guidelines TR-03110: ***Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC)***. Version 1.11, 2008

[20] BSI TR-03105 Part 5.1: ***Test plan for ICAO compliant Inspection Systems with EAC,*** Version 1.2, 2009

[21] NIST, ***Guide to Bluetooth security***: recommendations of the National Institute of Standards and Technology, Special Publication 800-121

[22] e-MOBIDIG, ***Identity on the Move***, http://www.e-mobidig.eu

[23] e-MOBIDIG , ***e-MOBIDIG Use Cases***, http://www.e-mobidig.eu

[24] e-MOBIDIG, ***e-MOBIDIG Country Examples***, http://www.e-mobidig.eu

[25] e-MOBIDIG , ***e-MOBIDIG Technical Guide***, http://www.e-mobidig.eu

[26] e-MOBIDIG , ***e-MOBIDIG Standards***, http://www.e-mobidig.eu

[27] Barbeu, M., ***Assessment of the True Risks to the Protection of Confidential Information in the Wireless Home and Office Environment***, pp.1-6, 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2010

[28] ***Integrated Risk Management Framework (IRMF)***, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12254

[29] Mark Rounds, Norman Pendgraft, ***Diversity in Network Attacker Motivation: A Literature Review***, cse, vol. 3, pp.319-323, 2009 International Conference on Computational Science and Engineering, 2009

[30] ISO/IEC 7498-1:1994, Ed. 2 Information technology –***Open Systems Interconnection – Basic Reference Model***: The Basic Model

[31] ICAO TR – ***Supplemental Access Control for Machine Readable Travel Documents***, version 1.00 , 23 march 2010

[32] R. Cappelli, M. Ferrara and D. Maltoni, ***On the Operational Quality of Fingerprint Scanners***, IEEE Transactions on Information Forensics and Security, vol.3, no.2, pp.192-202, June 2008.

[33] A. Alessandroni, R. Cappelli, M. Ferrara and D. Maltoni, ***Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality***, in proceedings European Workshop on Biometrics and Identity Management (BIOID 2008), Roskilde, Denmark, pp.29-35, May 2008

[34] EU, DG JLS, ***VIS-NIST Description***, v. 1.23, February 2009

[35] EBTS, ***Electronic Biometric Transmission Specification (EBTS)***, document number IAFIS-DOC 01078-9.2, Federal Bureau of Investigation, May 2011

[36] ENISA, ***Privacy Features of European eID Card Specifications***, January 2009, http://www.enisa.europa.eu

[37] PIV, ***Personal Identity Verification: Image Quality Specifications for Single Finger Capture Devices***, FBI PIV-071006, July 2006

[38] BSI TR-03104, ***Technical Guideline for production data acquisition, -quality testing and transmission for official documents***, v. 2.1.5, October 2010

[39] Nill N.B. ***Test Procedures for Verifying IAFIS Image Quality Requirements for Fingerprint Scanners, V 1.1***, MITRE Technical Report 05B0000016R1, September 2008.

[40] Nill N.B., ***Test Procedures for Verifying Image Quality Requirements for Personal Identity Verification (PIV) Single Finger Capture Devices***, MITRE Technical Report MTR 060170, December 2006.

[41] NIST (2003), ***Fingerprint Vendor Technology Evaluation (FpVTE)***, http://fpvte.nist.gov/

[42] NIST (2003-2010), ***Proprietary Fingerprint Template (PFT) Evaluation***, http://www.nist.gov/itl/iad/ig//pft_2003.cfm

[43] Biometric Systems Lab University of Bologna (2000-2006), ***Fingerprint Verification Competition (FVC)***, http://biolab.csr.unibo.it/home.asp

[44] ISO/IEC 19795 — consists of seven parts, under the general title ***Information technology - Biometric performance testing and reporting***

[45] Biometric Systems Lab University of Bologna ***FVC on-going***, https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

[46] ICAO - ***RF protocol and application test standard for e-passport – Part 2 tests for air interface, initialisation, anti-collision and transport protocol***, Version: 1.02, February, 2007

[47] ICAO - ***RF protocol and application test standard for e-passport – Part 3 Tests for application protocol and logical data structure***, Version: 1.01, February, 2007

[48] ICAO - ***RF protocol and application test standard for e-passport - Part 4 e-passport reader tests for air interface, initialisation, anti-collision and transport protocol***, Version: 1.01, February, 2007

[49] ICAO, ***Guide to Interfacing e-MRTDs and Inspection Systems*** – Version 1.0, February, 2005

[50] Chris Roberts, ***Biometric attack vectors and defences, Computers & Security***, Volume 26, Issue 1, February 2007, Pages 14-25, ISSN 0167-4048

[51] IDABC, ***eID Interoperability for PEGS, Analysis and Assessment of similarities and differences – Impact on eID interoperability***, November 2007, http://ec.europa.eu/idabc/servlets/Doc0939.pdf?id=29618

[52] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- ***Evaluation criteria for IT security -- Part 1: Introduction and general model*** (Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model)

[53] ISO/IEC 15408-2:2008 Information technology -- Security techniques -- ***Evaluation criteria for IT security -- Part 2: Security functional components*** (Common Criteria for Information Technology Security Evaluation Part 2: Security functional components)

[54] ISO/IEC 15408-3:2008 Information technology -- Security techniques -- ***Evaluation criteria for IT security -- Part 3: Security assurance components*** (Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components)

[55] Common Methodology for Information Technology Security Evaluation: ***Evaluation methodology***, July 2009

[56] Rouchouze, B., ***Terminals for mobile eVerifications,*** Eurosmart, April 2011

APPENDIX: ABBREVIATIONS AND ACRONYMS

AA	Active Authentication
AFIS	Automated Fingerprint Identification System
BAC	Basic Access Control
BIG	Brussels Interoperability Group
BMS	Biometric Matching System
BPR	Best Practice Recommendations
BSI	Bundesamtes für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BSP	Biometric Service Provider
CC	Common Criteria
CEM	Common criteria Evaluation Methodology
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DG(n)	Data Group (n)
DS	Document Signer
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DV	Document Verifier
EAC	Extended Access Control
ECDSA	Elliptic Curve DSA
EF	Elementary File
ETSI	European Telecommunications Standards Institute
EU	European Union
FAR	False Accept Rate
FRR	False Reject Rate
FTE	Failure to Enrol Rate
IAFIS	Integrated Automated Fingerprint Identification System
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation

ID	Identifier
ISO	International Standards Organisation
IPSC	Institute for the Protection and Security of the Citizen
IQS	Image Quality Specifications
IS	Inspection System
ITSEC	Information Technology Security Evaluation Criteria
JRC	Joint Research Centre
LAN	Local Area Network
LDS	Logical Data Structure
MOBIDIG	MOBile Identification Interoperability Group
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NIST	National Institute for Standards and Technology
NFIQ	NIST Fingerprint Image Quality
OCR	Optical character Recognition
OSI	Open Systems Interconnection
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PDA	Personal Digital Assistant
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PP	Protection Profile
RF	Radio Frequency
RFID	Radio Frequency IDentification
RSA	Rivest, Shamir and Adleman
SAC	Supplemental Access Control
SCIC	Secure Contactless Integrated Circuit
SSL	Secure Socket Layer
SOD	Security Data Object
SPOC	Single Point Of Contact
ST	Security Target

TCSEC	Trusted Computer System Evaluation Criteria
TESTA	Trans European Services for Telematics between Administrations[20]
TETRA	Terrestrial Trunked Radio
TLS	Transport Layer Security
TOE	Target Of Evaluation
USB	Universal Serial Bus
VIS	Visa Information System
VPN	Virtual Private Network
XML	eXtensible Markup Language
WG	Working Group

[20] Private IP-based network of the European Union.

European Commission

EUR 25037 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Mobile Identification:from Functional Requirements, to Testing for Interoperability and Security
Authors: Antonia Rana, Alessandro Alessandroni
Luxembourg: Publications Office of the European Union
2011 – 88 pp. – 21x29,7 cm
EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)
ISBN 978-92-79-22060-9
doi:10.2788/10498

Abstract
The present document provides an analysis of the technical, functional and interoperability requirements for a generic mobile identification solution.
The report starts from the findings and discussions held so far in the context of the e-MOBIDIG working group, defines a high-level abstract architecture for a mobile identification device, identifying its main components. It then analyses available standards, conformity tests for each of the components with a particular view to security and interoperability. Existing guidelines and recommendations from international organisations are also taken into account in the analysis and discussions.
From the analysis of the experiences and discussions in the e-MOBIDIG working group, it emerges that use cases and contexts are different and there is no "ideal solution" which fits all cases. At the same time, the market offers already numerous solutions which are able to accommodate the numerous scenarios that are conceivable in the context of identification and authentication using a mobile setting.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-25037-EN-N

ISBN 978-92-79-22060-9